THREAT HUNTER RESEARCH

2024 Annual Cybercrime Ecosystem Trends Report

An annual view of changing attack resources, identity and cloud abuse, and seven major fraud scenarios observed in 2024.

Original publication: 2025-01-16
Research team: Threat Hunter Research Team
Source report: 81 pages

Original report text

This text version is reconstructed based on the 81-page original PDF, retaining the report narrative, chapters and research scope; the cover, repeated table of contents and purely decorative pages are not repeated. Localized figures are placed in context throughout this web edition, with the original PDF retained for reference.

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 named a representative vendor in leading industry analysts' technology maturity and threat intelligence reports 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 2024, cybercriminal attacks on the Internet remained severe. No matter in terms of the size of cybercriminal groups, or the evolution of attack resources, attack technology applications, and attack scenarios, there have been major changes.

In terms of attack resources, Threat Hunter captured more than 16 million new malicious phone numbers around the world in 2024, and 11.7 million daily active malicious IPs, a significant increase from 2023. In order to avoid fraud-control monitoring, cybercrime ecosystem continues to upgrade its technology to find more covert attack resources, such as implanting Trojans in normal user equipment and using their IP as attack resources, and the rapid development of the "merchant money laundering" industry chain.

In terms of attack technology, threat-actor groups have also made new developments in the application of general technologies in 2024, such as abusing "sub-master machines" to bypass identity authentication, using "NFC remote transmission software" for cross-border money laundering, customized cloud mobile phone systems to improve attack efficiency, etc.

In terms of attack scenarios, online business fraud, financial loan fraud, brand advertising fraud, API attacks, phishing and counterfeiting, data leakage, telecommunications network fraud and other scenarios continue to become more popular. Online business fraud has entered deep water, with indiscriminate attacks on all industries and all business links; the Wang Xing incident has further heightened public attention to telecommunications network fraud.

Threat Hunter released the "2024 Internet fraud network Research Report". Based on in-depth research on the Internet's fraud network in 2024, it analyzes attack resources used by cybercriminal groups, attack technologies, attack scenarios and other dimensions in 2024, and objectively presents the overall development trend of the Internet cybercrime ecosystem in 2024.

It aims to help enterprises from all walks of life improve their understanding of the cybercrime ecosystem from the intelligence dimension, thereby further improving fraud-control strategies.

Table of Contents About Threat Hunter Preface 1. Analysis of attack resources used by cybercriminal groups on the Internet in 2024

1. 1 Analysis of malicious mobile-number resources in 2024

1. 2 Analysis of malicious IPs resources in 2024

1. 3 Analysis of Internet Money Laundering Resources in 2024

1. 4 Analysis of risk mailbox resources in 2024

2. Analysis of common cybercriminal groups attack technologies on the Internet in 2024

2.1 Evolution of identity bypass technology: threat actors use "sub-master machines" to bypass authentication, and unqualified personnel can also take orders on the platform

2.2 threat actors use "NFC" remote transmission software to launder money across borders and move illegal funds

2. 3 Customized cloud mobile phone system to further improve the attack efficiency of threat actors

3. Analysis of cybercriminal groups attack scenarios on the Internet in 2024

3. 1 Online business fraud scenarios

3. 2 Financial loan fraud scenarios

3. 3 Brand advertising fraud scenarios

3. 4 API attack scenarios

3. 5 Phishing and Counterfeiting Scenarios

3. 6 Data Leakage Scenarios

3. 7 Telecom network fraud scenarios

Write at the end

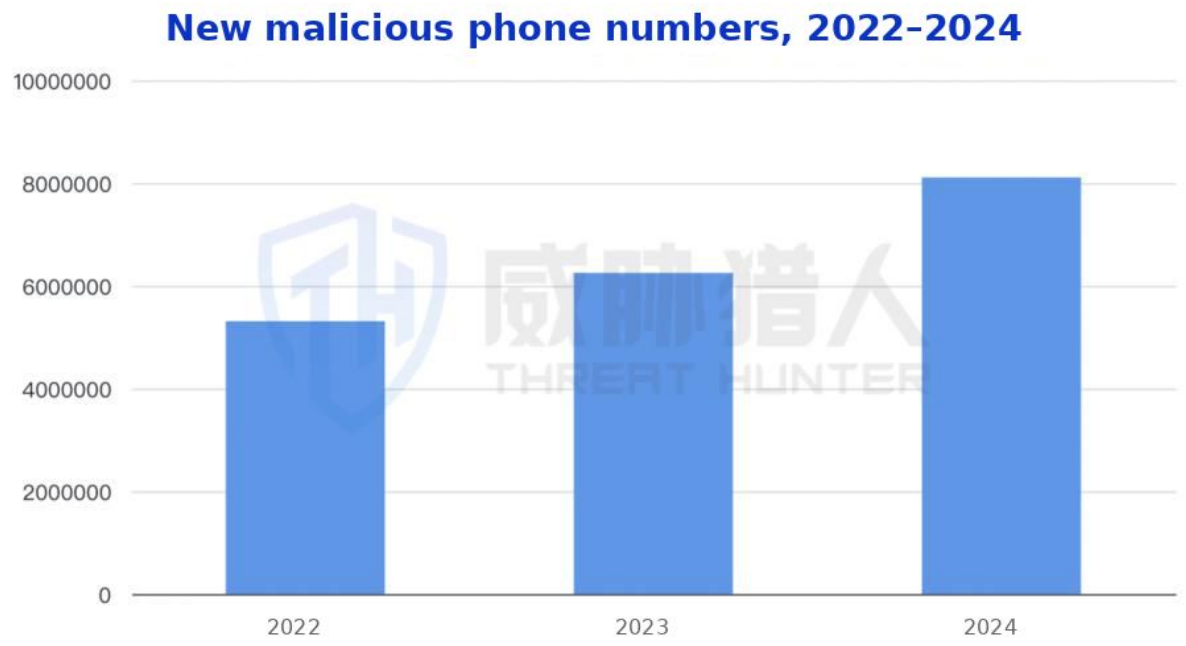
Analysis of Internet attack resources used by cybercriminal groups in 2024

1. Analysis of attack resources used by cybercriminal groups on the Internet in 2024

1.1 Analysis of malicious mobile-number resources in 2024

1.1.1 The number of new domestic malicious phone numbers exceeded 8 million in 2024, an increase of 30% compared with 2023

According to Threat Hunter intelligence data, the number of domestic malicious phone numbers has continued to rise in recent years, with new additions exceeding 8 million in 2024, an increase of 30% from 2023.



New malicious phone numbers, 2022–2024

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

Among the malicious mobile-number resources, "SIM pool cards" and "Interception Card" account for the highest proportion. The following sections 1.1.2 and 1.1.3 will focus on analyzing the changes in the resources of "SIM pool cards" and "Interception Card" in 2024.

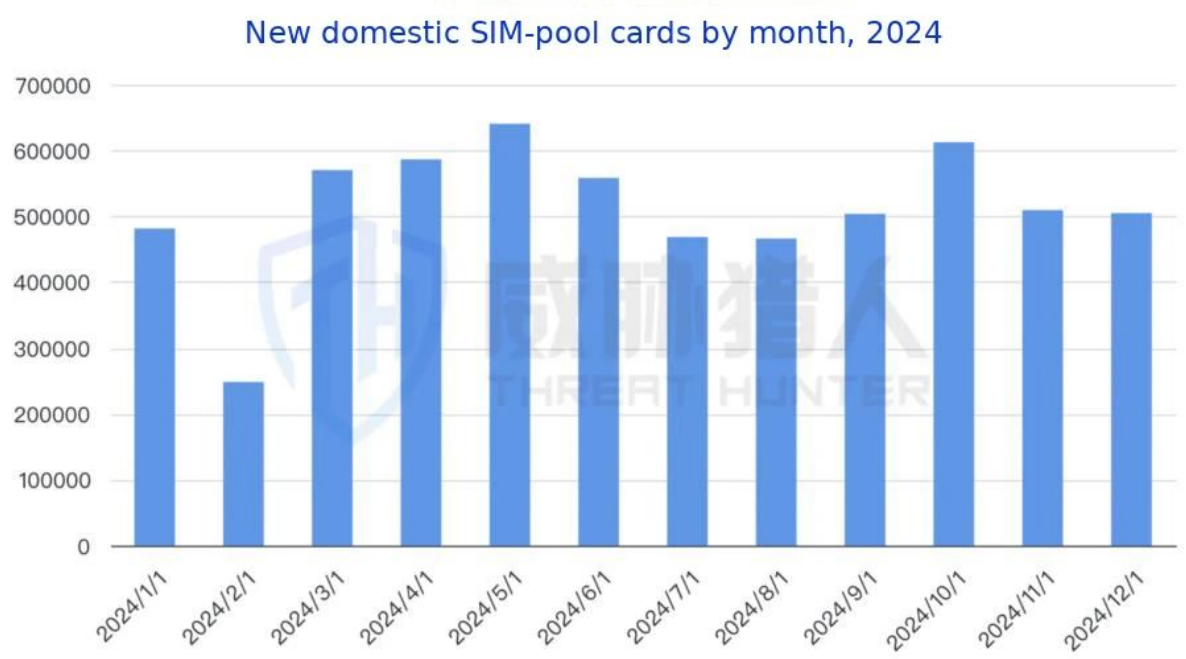
1.1.2 Analysis of "SIM pool cards" Resources in 2024

(1) There were 6.15 million new SIM pool cards in China in 2024, an increase of 4.86% compared with 2023

According to Threat Hunter intelligence data, there were 6.15 million new SIM pool cards in China in 2024, an increase of 4.86% from 2023.

SIM pool cards: refers to an malicious activity mobile phone card that uses the "SIM pool" network communication hardware to realize simultaneous calls to multiple numbers, group text messages and other functions.

Judging from the changing trend of the number of domestic SIM pool cards in 2024, from February, June to September, the number of new domestic SIM pool mobile phone cards showed a downward trend.



New domestic SIM-pool cards by month, 2024

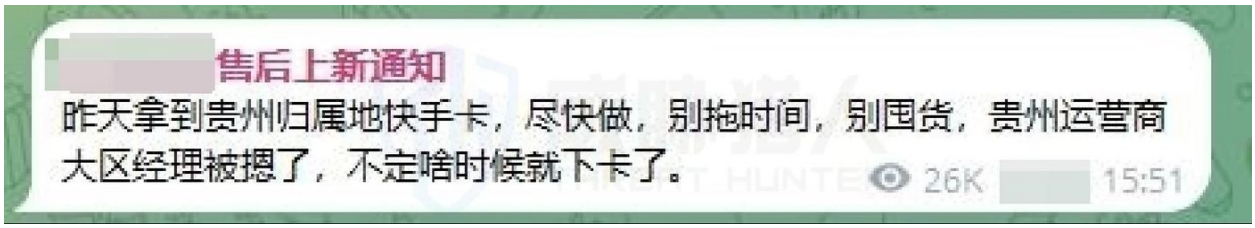
Source: Threat Hunter original report, page 7. Original figure with Chinese text replaced by English.

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

1. In February, due to the slowdown in transactions of threat actors during the Spring Festival, the number of attackers decreased significantly, and the steady upward trend resumed after the holiday;

2. From June to September, due to the intensified crackdown by regulatory agencies, many card issuing platforms were shut down and some card dealers were arrested, resulting in a reduction in supply.

This resulted in a decrease in the number of new SIM pool cards.



Card dealer notice: newly issued cards from one province should be used quickly

Source: Threat Hunter original report, page 7. Original image retained.

(2) Top 3 provinces to which newly added SIM pool cards will belong in China in 2024: Shanghai, Beijing, Liaoning

Threat Hunter intelligence data statistics show that the provinces (including municipalities) where new SIM pool cards was added in China in 2024 will mainly be concentrated in Shanghai, Beijing, and Liaoning Province.

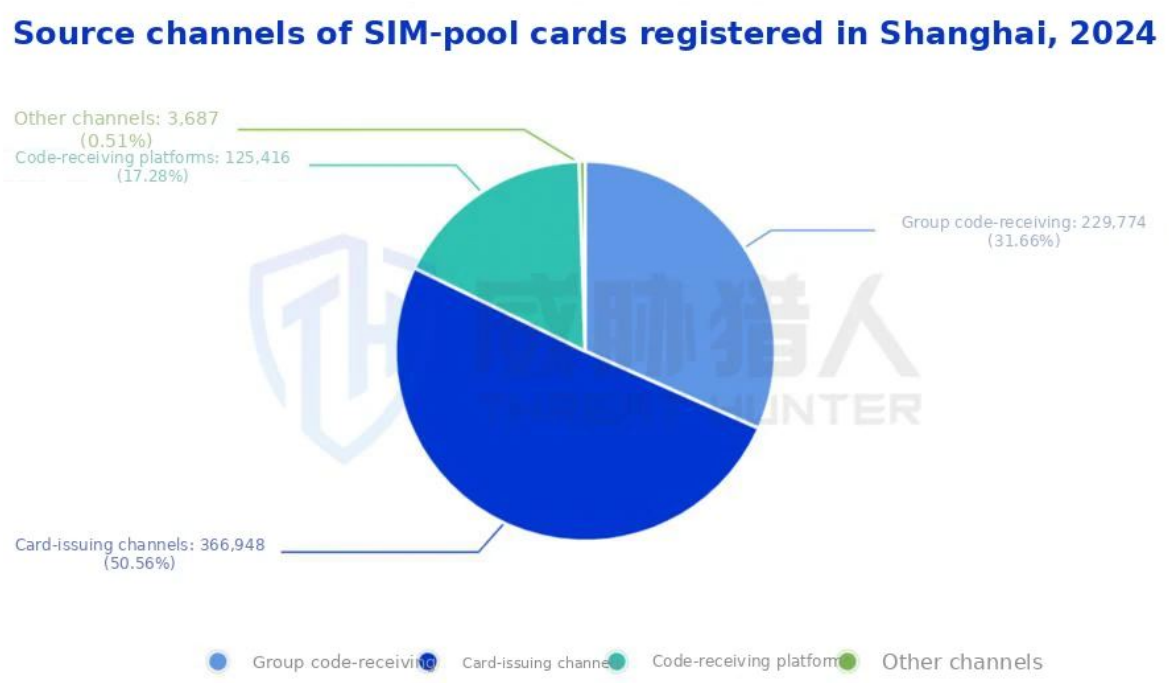


Top 10 provinces for new SIM-pool cards, 2024

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

Among them, the number of SIM pool cards located in Shanghai increased by 87.86% year-on-year in 2023. Threat Hunter noticed that the number of SIM pool cards in Shanghai this year has remained relatively high in every month throughout the year, and leading card merchants active on the card issuance platform have also continued to provide Shanghai SIM pool cards this year.

Through the analysis of the source channels of SIM pool cards newly added in Shanghai this year, it was found that the number of SIM pool cards from card issuing platforms accounted for more than half:



Source channels of SIM-pool cards registered in Shanghai, 2024

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

The changes in the top 10 locations of newly added SIM pool cards in China in 2024 compared to 2023 are as follows:

Province	2024 rank (new SIM-pool cards)	Change vs 2023
Shanghai	1	Up 3
Beijing	2	Up 7
Liaoning	3	Up 2
Shandong	4	Down 2
Hebei	5	Up 1
Guangdong	6	Up 2
Jiangsu	7	Down 6
Hubei	8	Not in 2023 top 10
Fujian	9	Not in 2023 top 10
Chongqing	10	Unchanged

Top 10 provinces for new SIM-pool cards, 2024, and change from 2023

Source: Threat Hunter original report, page 9. Table re-typeset in English from the original.

[Attention] Malicious phone numbers originating in Hong Kong, China, continued to grow in 2024, with 782,500 cases captured throughout the year. It is worth noting that Threat Hunter intelligence data shows that since March 2024, the number of risky mobile phone card transactions originating in Hong Kong, China has increased significantly, reaching a peak in September.

Due to the strong demand from downstream fraudsters, Hong Kong phone numbers are still in large demand by threat actors because they can be registered for domestic and foreign applications, are low-cost, and have long availability.



Trading intelligence on Hong Kong risk SIM cards by quarter, 2024

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

Compared with other domestic mobile phone cards, China Hong Kong mobile phone cards have the following characteristics:

1. Wide range of registration: Hong Kong mobile phone cards have a wide range of registration, and can be used to register domestic and international messaging apps;

2. Long online usage time: The online usage time of Hong Kong mobile phone card verification-code reception service is longer than that of other domestic cards. Generally, one can be guaranteed

It can be used repeatedly every month, while other domestic mobile phone cards are generally valid for several days;

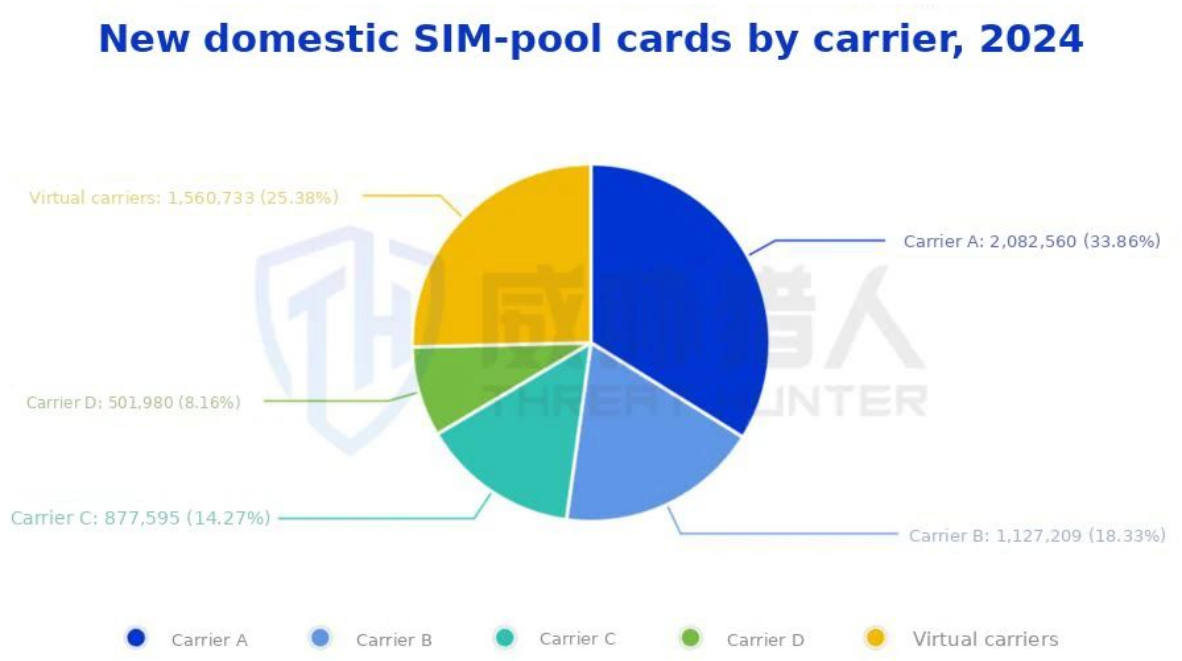
3. Lower price: The price of Hong Kong mobile phone cards is lower than the price of other domestic cards;

4. Supports multiple verification-code reception forms: Hong Kong cards support multiple verification-code reception forms. Threat Hunter currently sees them offered on SMS verification-code receiving platforms, card-issuing websites, and private-domain code-receiving channels.

Threat Hunter has found malicious-activity records involving Hong Kong phone cards in all of these channels.

(3) In 2024, 76.42% of new domestic SIM pool cards will be owned by the three major operators, an increase of 14.51% compared with last year. Threat Hunter intelligence data shows that the operators of newly added domestic SIM pool cards this year are mainly basic operators, accounting for 76.42%, an increase of 14.51% compared with last year.

Threat Hunter intelligence personnel found through research that the proportion of the three major operators has increased this year, mainly because many companies have further improved fraud controls on virtual operator mobile phone cards, resulting in an increase in threat actors' demand for mobile phone card resources from the three major domestic operators.



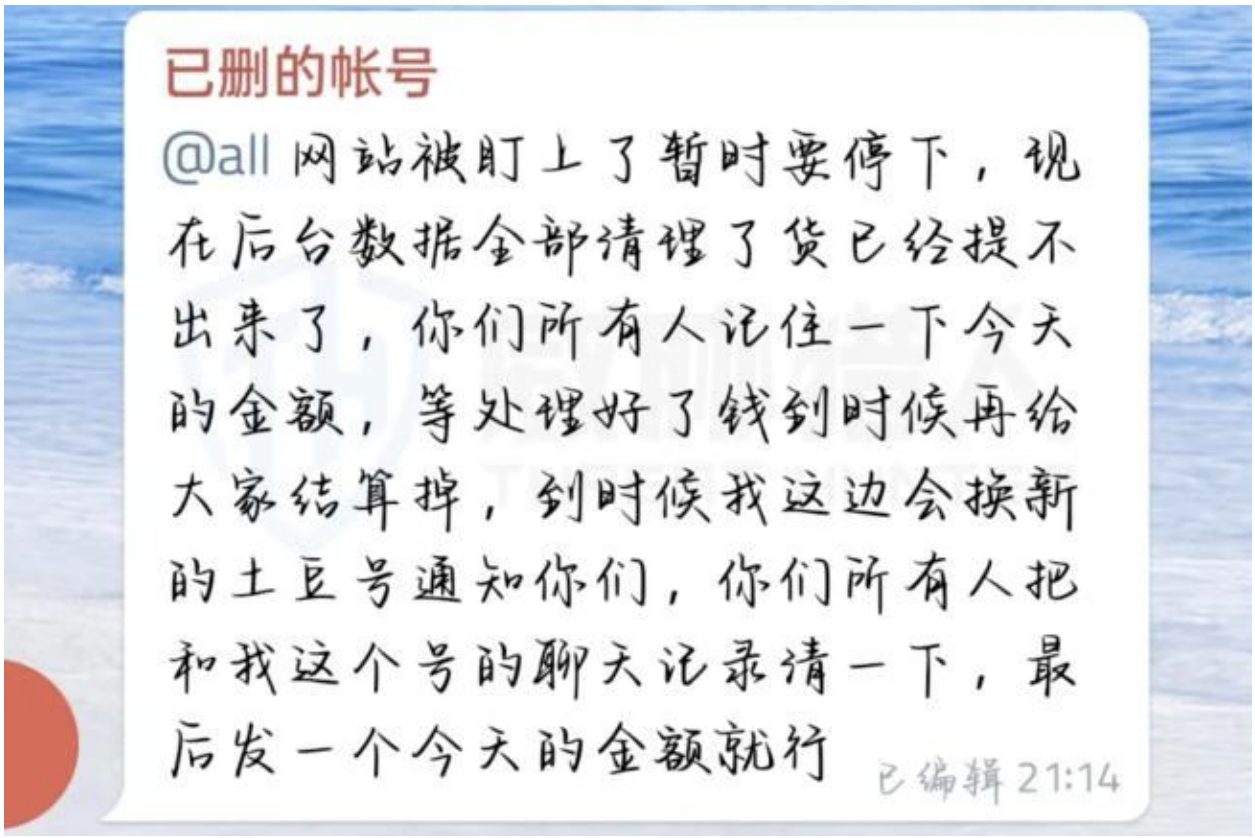
New domestic SIM-pool cards by carrier, 2024

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

(4) [Attention] The number of SIM-pool card card issuance platforms increased by 39.37% in 2024, but the platform life cycle was shortened. Threat Hunter continued to monitor the changing trends of cybercrime ecosystem malicious resources source channels and found that the number of SIM-pool card card issuance platforms, the main contribution channel, increased significantly in 2024, but the life cycle was shortened:

There were 171 new SIM pool cards issuance platforms in 2024, with a simultaneous growth of 39.37% in 2023, but 24% of them have been operating for less than a week. Threat Hunter further investigated and found that card-issuing platforms have suffered strong regulatory pressure this year. Many card-issuing platforms and active SIM pool cards dealers have ceased operations or been active due to regulatory crackdowns.

In addition, Threat Hunter tested the currently surviving SIM pool cards-related card issuance platforms and found that some cybercrime operators will take some higher security measures in order to prevent regulatory crackdowns, including but not limited to periodic order deletion, use of cryptocurrency payments, frequent changes to verification-code reception addresses, and restrictions on abnormal access and payments.



Notice from a SIM-pool card platform announcing it was shutting down

Source: Threat Hunter original report, page 11. Original image retained.

1.1.3 Analysis of “Interception Card” Resources in 2024

(1) There were 1.96 million new interception cards in the country in 2024, an increase of 405.50% over 2023. According to Threat Hunter intelligence data, there were a significant increase in new interception cards in the country in 2024, with a total of 1.9664 million cases, an increase of 405.50% over 2023.

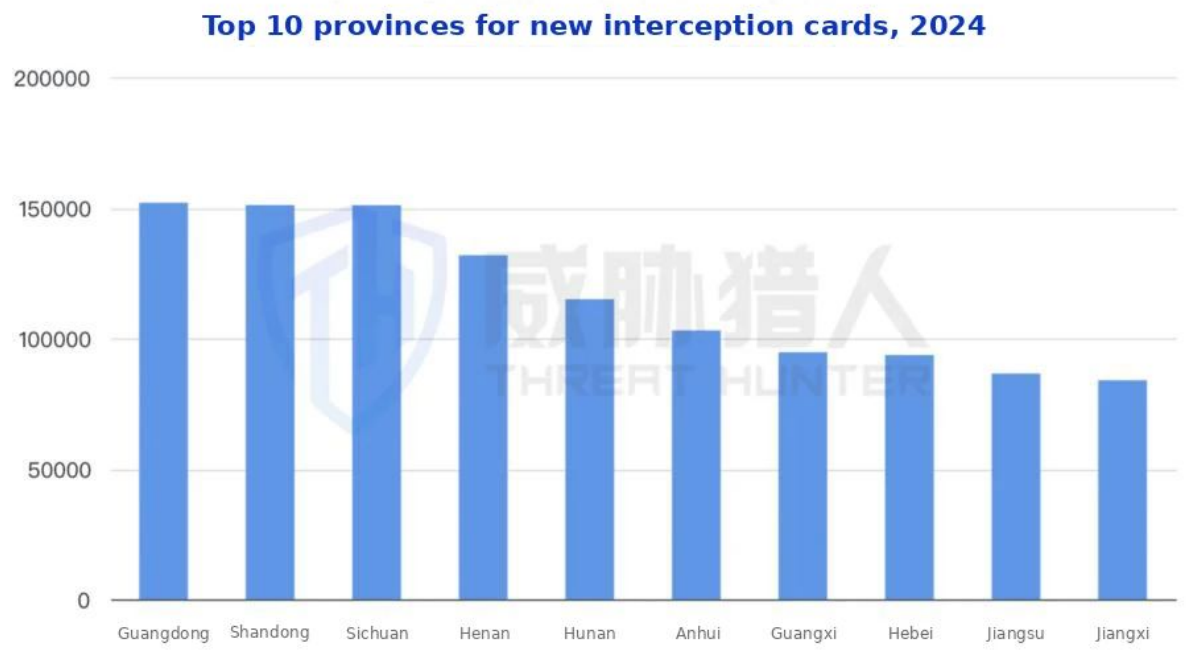
Threat Hunter research found that the significant increase in the number of interception cards in January was due to a new interception card channel that emerged at the end of last year and invested a large amount of interception card resources. In 2024, this channel contributed nearly one million interception cards, accounting for 48.82% of the overall number this year. However, the channel was inactive from June to July 2024, and finally ceased operations in December 2024.



New domestic interception cards by month, 2024

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

(2) Top 3 provinces to which new interception cards was added in the country in 2024: Guangdong, Shandong, and Sichuan Threat Hunter intelligence data statistics show that the provinces (including municipalities) to which the new interception cards was added in the country in 2024 will mainly be concentrated in Guangdong, Shandong, and Sichuan.



Top 10 provinces for new interception cards, 2024

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

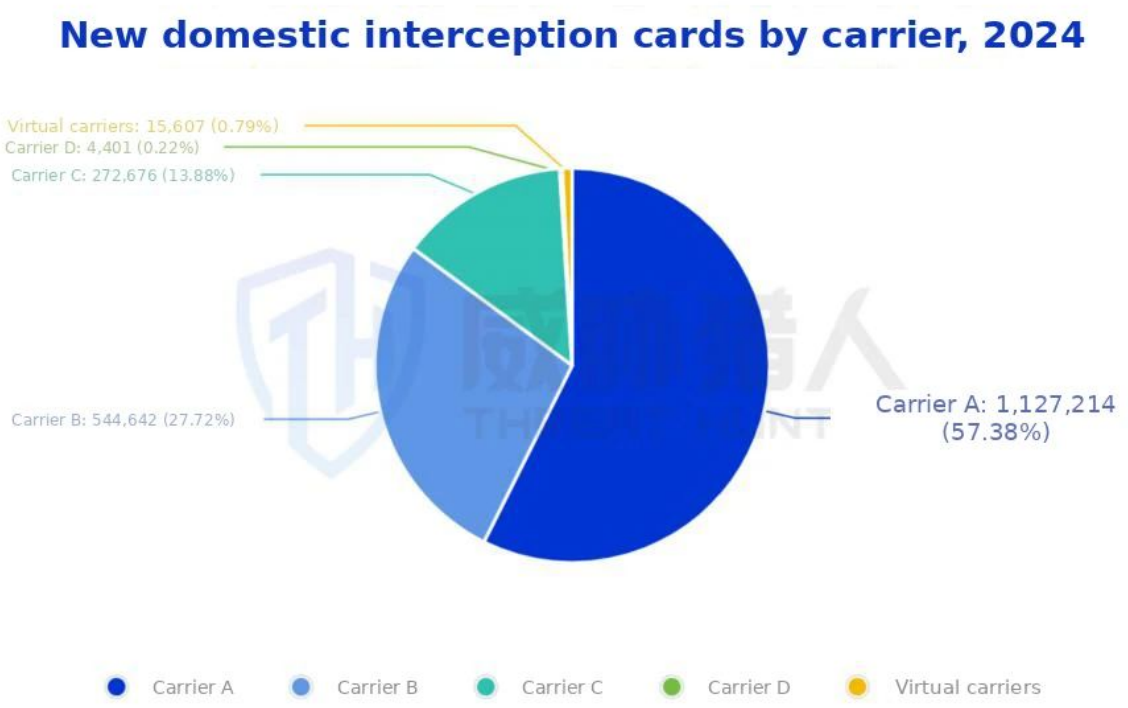
Comparison of the top 10 new domestic interception cards in 2024 with changes in 2023:

Province	2024 rank (new interception cards)	Change vs 2023
Guangdong	1	Up 3
Shandong	2	Unchanged
Sichuan	3	Up 4
Henan	4	Up 1
Hunan	5	Not in 2023 top 10
Anhui	6	Up 4
Guangxi	7	Down 6
Hebei	8	Unchanged
Jiangsu	9	Down 6
Jiangxi	10	Down 4

Top 10 provinces for new interception cards, 2024, and change from 2023

Source: Threat Hunter original report, page 13. Table re-typeset in English from the original.

(3) In 2024, 98.99% of new domestic interception cards will belong to the three major operators. Threat Hunter intelligence data shows that 98.99% of new domestic interception cards this year will belong to basic operators, and 1.01% will belong to other operators.



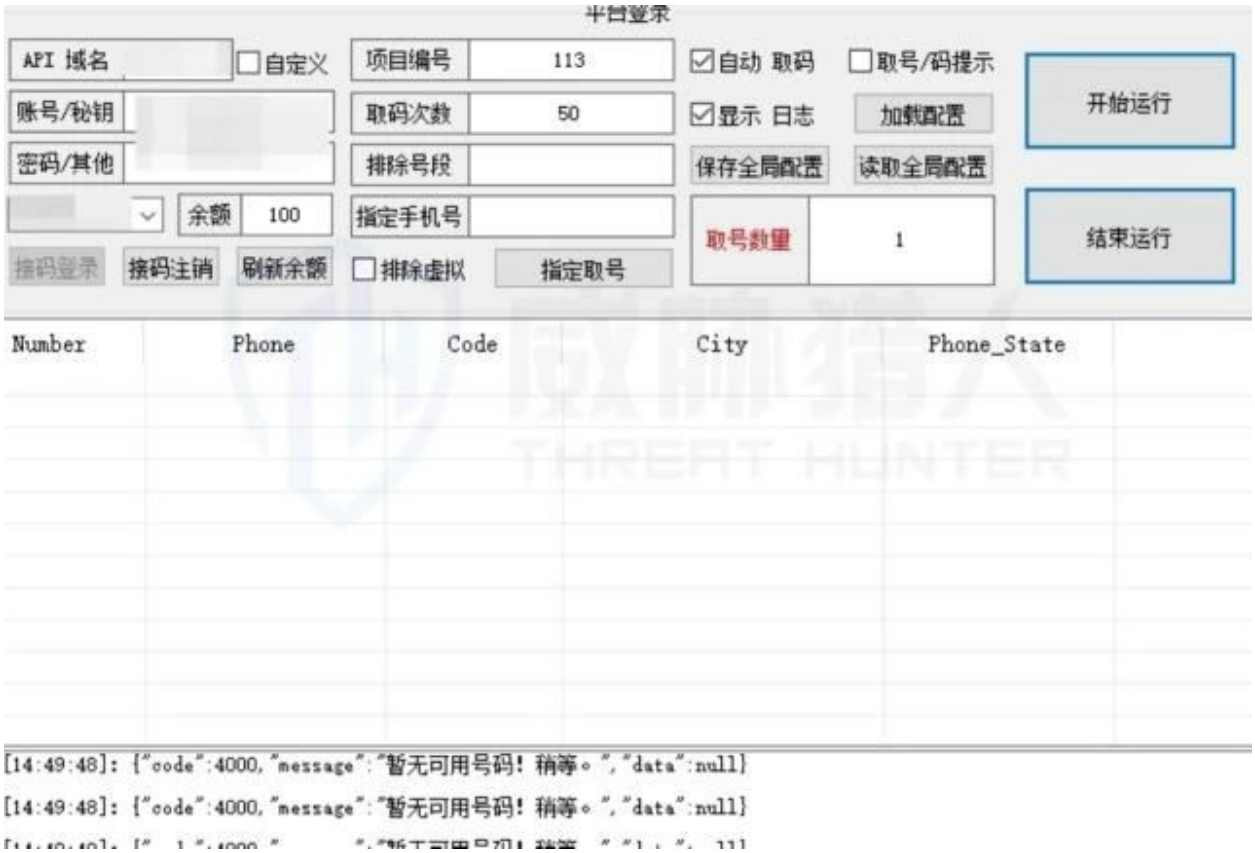
New domestic interception cards by carrier, 2024

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

(4) [Attention] The "Group Code Receiver" mode simplifies the process for threat actors to use interception cards, and makes the interceptor card's real platform more hidden. Threat Hunter research found that the interception card code reception method has gradually changed from the traditional interception card platform code reception mode to the "Group Code Receiver" mode.

In this mode, the interception card dealer hides the real number and only displays the coded number. Only buyers of illicit SIM cards can obtain the complete number to complete the code reception and conduct malicious activity.

Example of traditional interception card platform receiving code:



Code-receiving tool of a traditional interception card platform

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

Example of code reception in group code reception mode of "Interception Card"



Code receiving in the group code-receiving model

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

Compared with traditional interception card platforms that use exclusive verification-code reception tools to receive codes, the advantages of this model are:

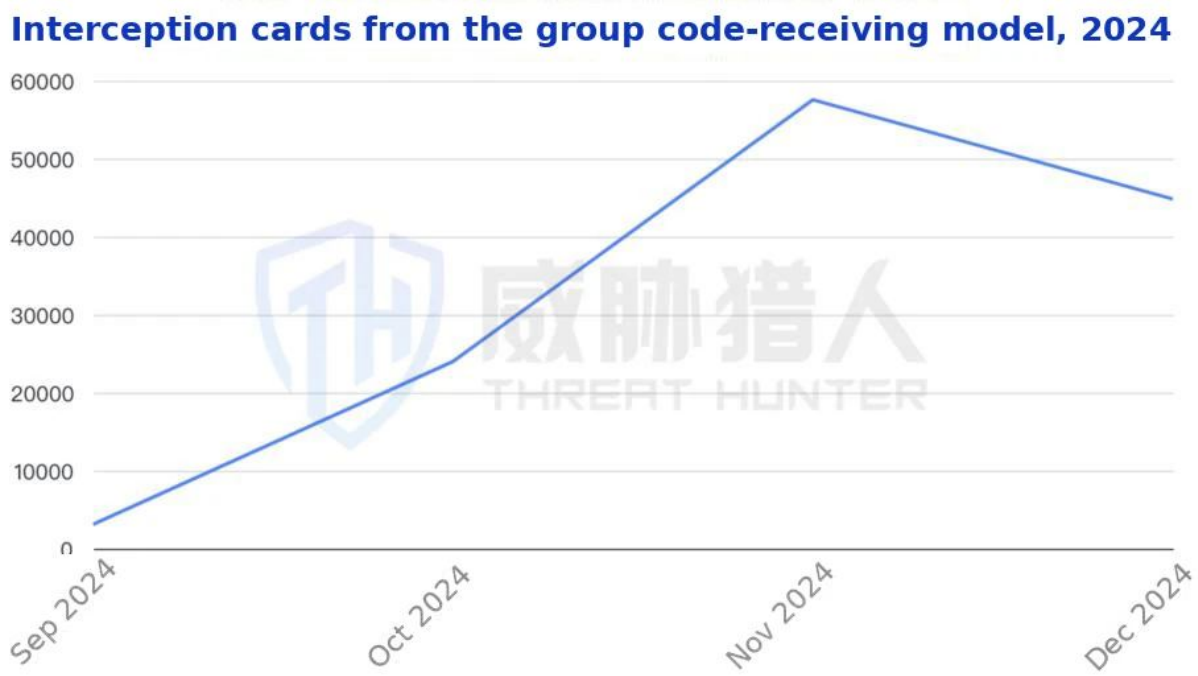
1. It is more convenient to use. Card merchants only need to provide numbers and code access links, and there is no need to open accounts or configure rights for downstream agents or illicit SIM-card users.

limited;

2. Higher concealment. Card merchants can hide the real platform information through the "group access code" mode and avoid exposing the platform's sensitive information to users.

user.

Currently, an average of 1,269 malicious SMS records are captured through the "Group Access Code" channel every day. The peak of malicious SMS records was in November, when nearly 60,000 malicious SMS records were captured:



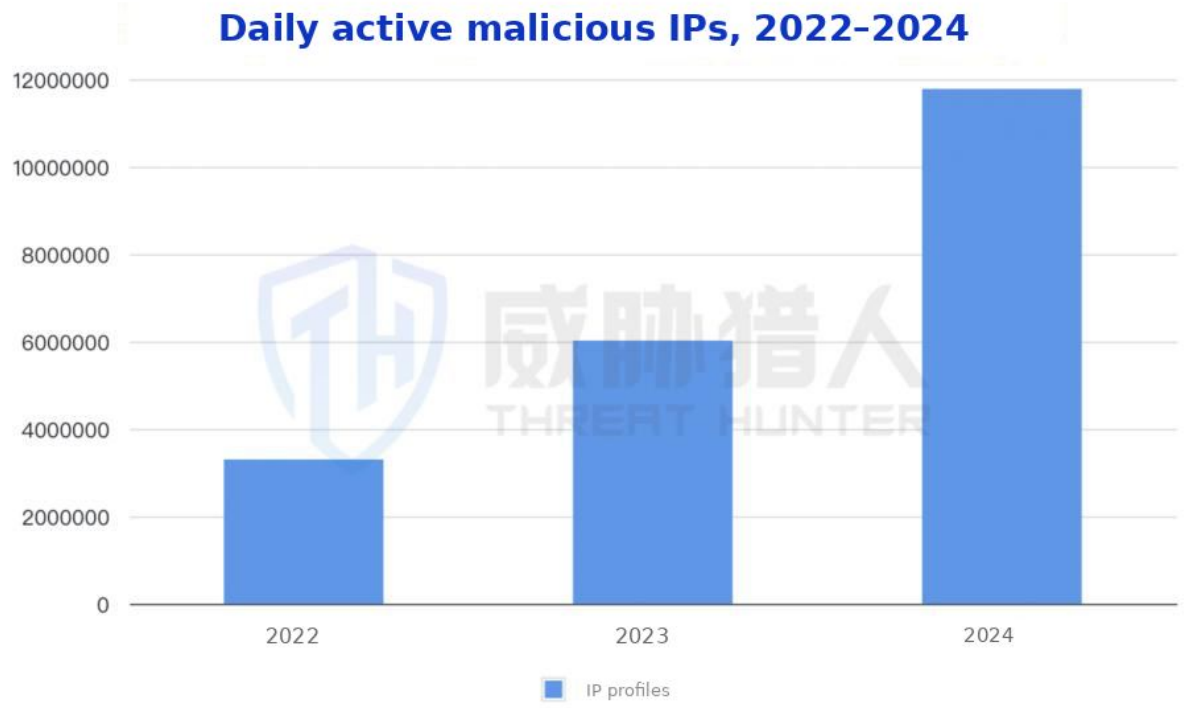
Interception cards from the group code-receiving model, 2024

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

1.2 Analysis of malicious IPs resources in 2024

1.2.1 There are 11.78 million daily active malicious IPs in 2024, an increase of 95.68% compared with 2023

According to Threat Hunter intelligence data, the number of daily active malicious IPs has continued to rise in recent years. In 2024, the number of daily active malicious IPs reached 11.78 million, an increase of 95.68% from 2023.

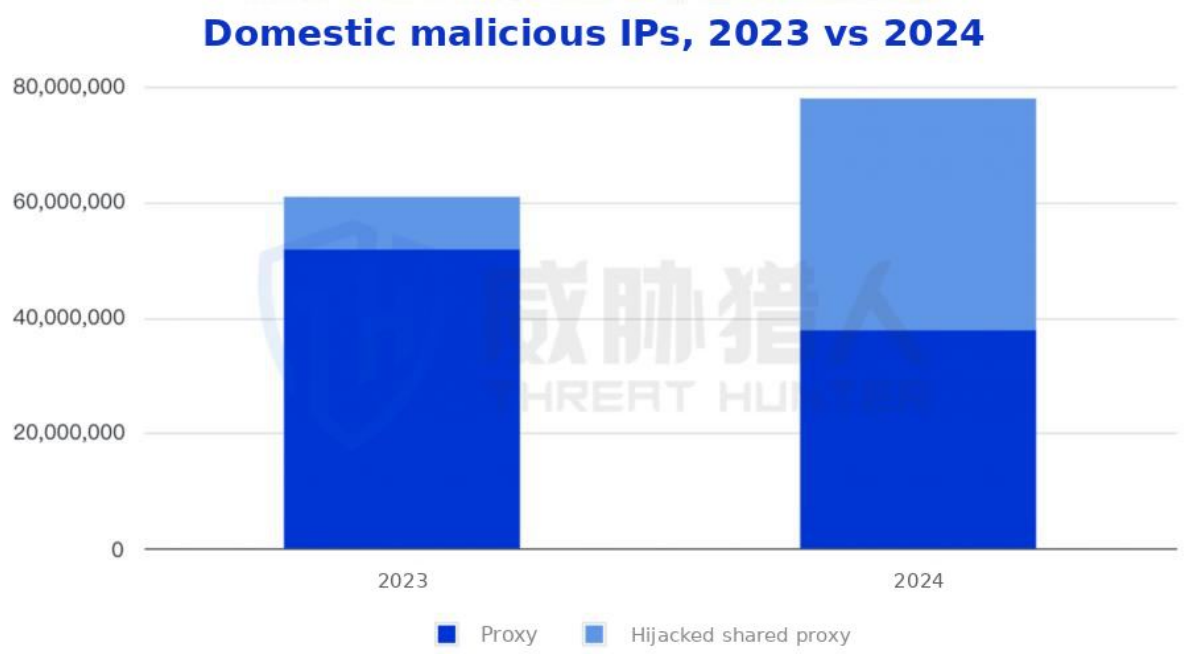


Daily active malicious IPs, 2022–2024

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

1.2.2 Analysis of domestic malicious IPs resources in 2024

(1) In 2024, there were 77.94 million domestic malicious IPs, a year-on-year increase of 31.96%. In 2024, Threat Hunter captured a total of 77.94 million domestic malicious IPs, a year-on-year increase of 31.96%.



Domestic malicious IPs, 2023 vs 2024

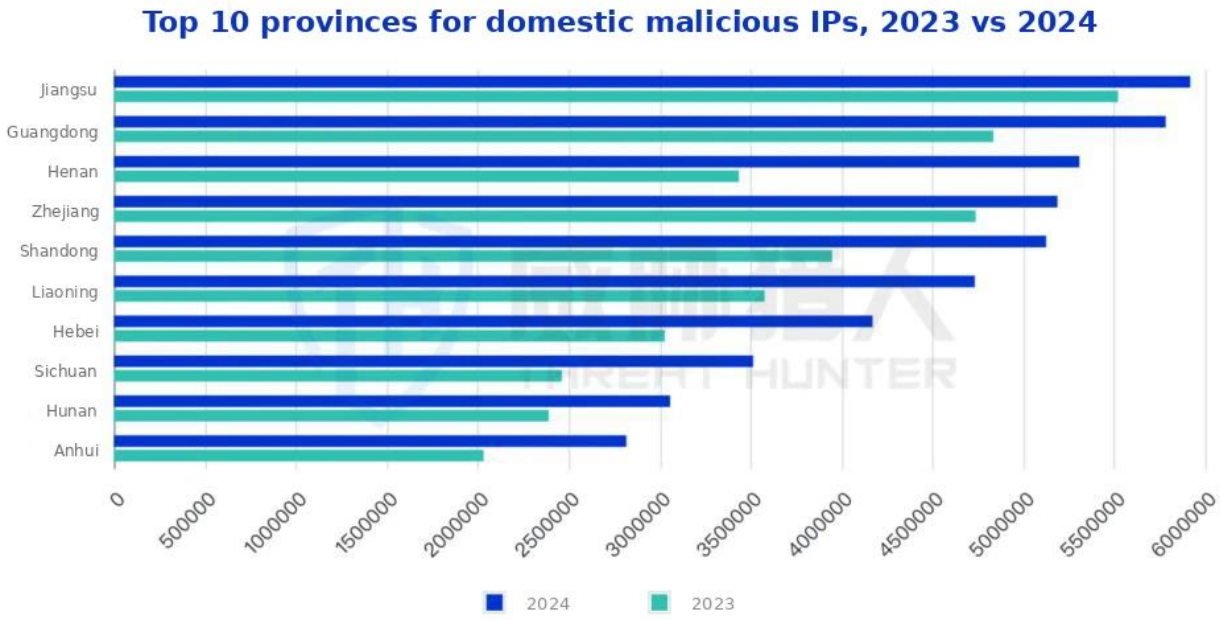
Source: Threat Hunter original report, page 17. Original figure with Chinese text replaced by English.

Threat Hunter research found that the substantial increase in domestic malicious IPs in 2024 is mainly caused by the rapid increase in the number of hijacked shared proxy IPs.

In 2024, the domestic hijacking shared proxy platform developed rapidly. Threat Hunter captured more than 40 million hijacked shared proxy IPs, accounting for 51.47% this year from 14.91% last year, and exceeded the proportion of ordinary proxy IPs.

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

In January 2024, Threat Hunter has marked this type of IP as a "hijacking shared proxy IP" risk label (2) Top 3 provinces where domestic malicious IPs belong in 2024: Jiangsu, Guangdong, and Henan. Threat Hunter intelligence data statistics show that in 2024, the active domestic malicious IPs provinces (including municipalities) are mainly concentrated in Jiangsu Province, Guangdong Province, and Henan Province. Among them, Henan Province has the largest increase in weight, increasing by 54.45%, and its ranking has also moved from sixth to third in 2023.



Top 10 provinces for domestic malicious IPs, 2023 vs 2024

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

(3) [Attention] threat actors' IP resource acquisition technology upgrades, using normal users' IP resources to avoid fraud-control detection. With the enhancement of network security supervision and corporate fraud-control strategies, in order to avoid fraud-control detection and tracking, threat actors are also upgrading their technology to try to mine more covert IP attack resources.

In recent years, Threat Hunter has successively discovered the types of malicious IPs used by normal users and criminals, conducted in-depth research on them, and launched risk labels such as "hijacking shared proxy IP", "cloud service IP", and "cloud mobile phone IP" in 2024.



Risk labels for IPs that normal users also share

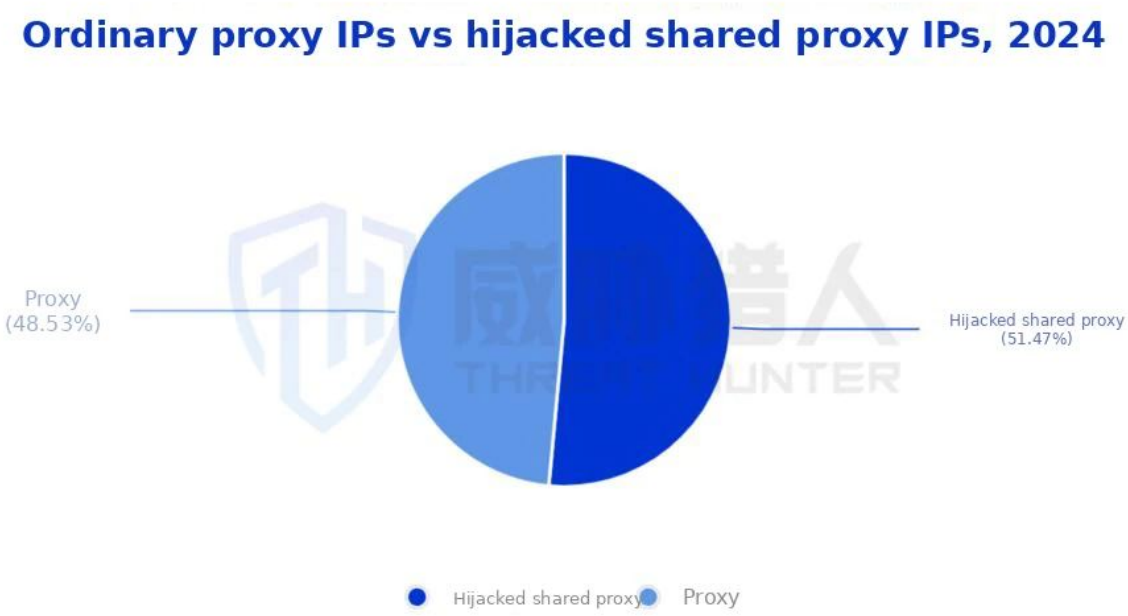
Source: Threat Hunter original report, page 18. Original figure with Chinese text replaced by English.

1. Hijacking shared proxy IPs accounted for more than half in 2024, becoming the main attack resource used by attackers

Hijacking shared proxy IP refers to normal user IP resources maliciously hijacked by threat actors. Threat Hunter found that threat actors implanted Trojans into normal user devices and used the Trojans to establish proxy channels on normal user networks. Each use time is very short, so it is difficult for ordinary users to perceive that their IP has been stolen.

Hijacking shared IPs is a normal behavior for normal users most of the time. Only a few times are hijacked by threat actors for short-term malicious behaviors. Therefore, platform fraud controls will directly treat them as normal users and ignore their short-term malicious activity behaviors. This makes the success rate of threat actors using hijacked shared IPs often higher than that of ordinary proxy IPs, leading to more and more platforms turning to hijacking shared proxy IP resources.

This type of hijacked shared proxy IPs appeared at the end of 2023, and developed rapidly in 2024, with a sharp increase in number. In 2024, Threat Hunter captured more than 40 million hijacked shared proxy IPs, a year-on-year increase of 341.81%, and exceeded the number of ordinary proxy IPs.



Ordinary proxy IPs vs hijacked shared proxy IPs, 2024

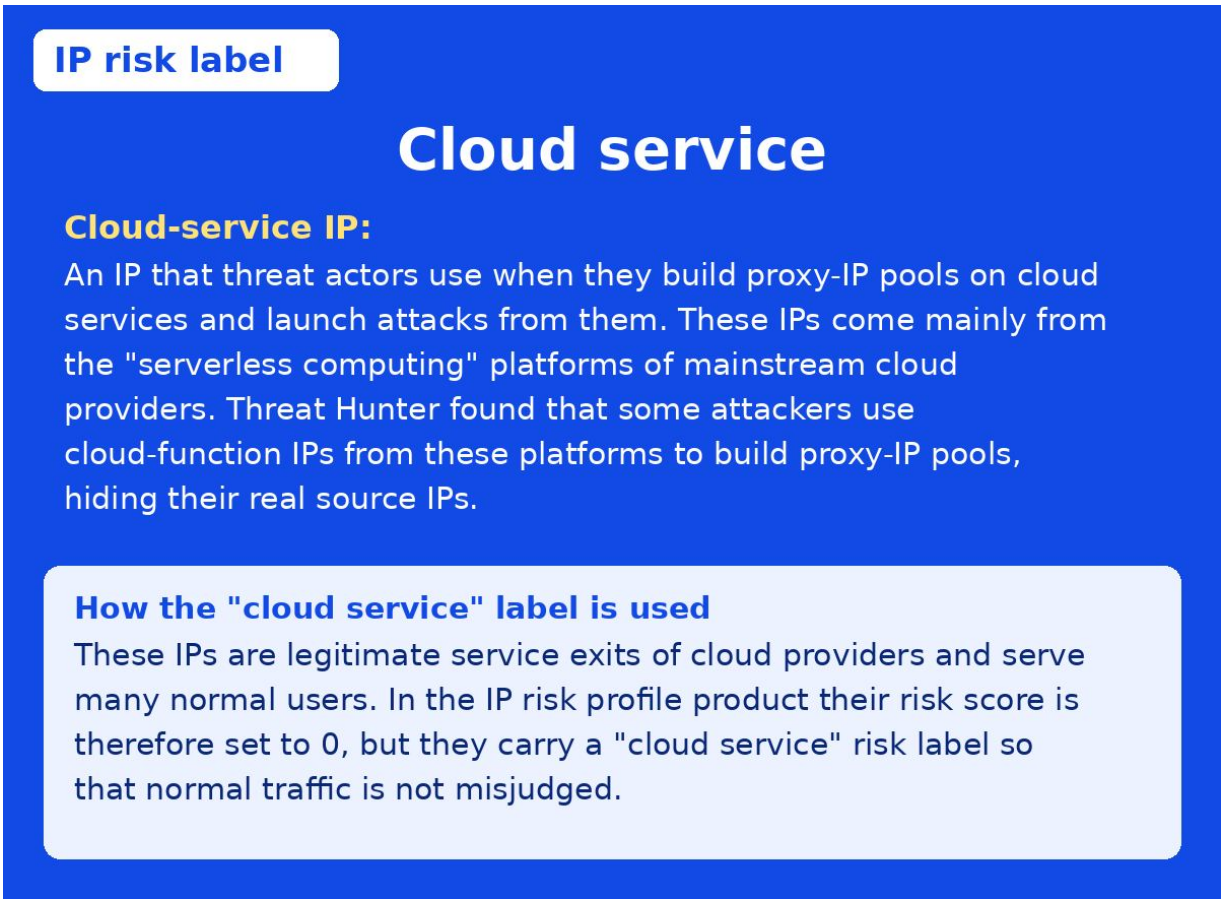
Source: Threat Hunter original report, page 19. Original figure with Chinese text replaced by English.

2. threat actors abuse cloud technology: Cloud functions and cloud mobile phone group control technology have become new ways for threat actors IP to conduct malicious activity.

While cloud service technology brings convenience to various industries, it is also being abused by threat actors. Some threat actors have turned the achievements of cloud technology into malicious tools, such as using cloud services to build proxy IP resource pools and using the group control settings of cloud phones to launch attacks on enterprises.

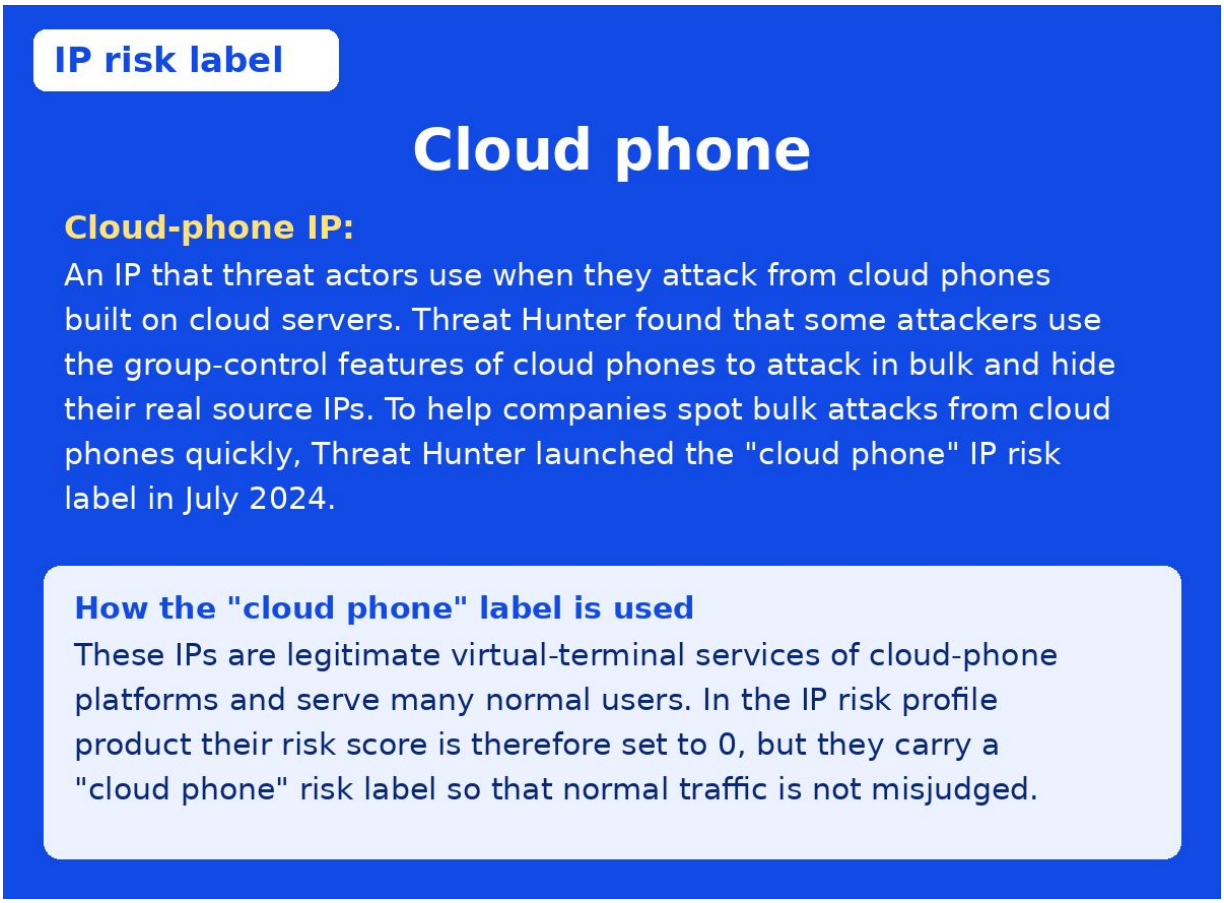
Threat Hunter found that in order to conceal the true source IP, some attackers would use the cloud function IP of the cloud computing platform to build a proxy IP pool to perform attacks, or use the group control configuration of cloud phones to perform batch attacks. Threat Hunter defined the IPs generated by these two methods as "cloud service IP" and "cloud phone IP."

Whether it is cloud service IP or cloud mobile phone IP, they all serve many normal users. Therefore, platform fraud controls will generally treat them as normal users and ignore their malicious activity behaviors.



IP risk label: cloud service

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



IP risk label: cloud phone

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

1.2.3 Analysis of foreign malicious IPs resources in 2024

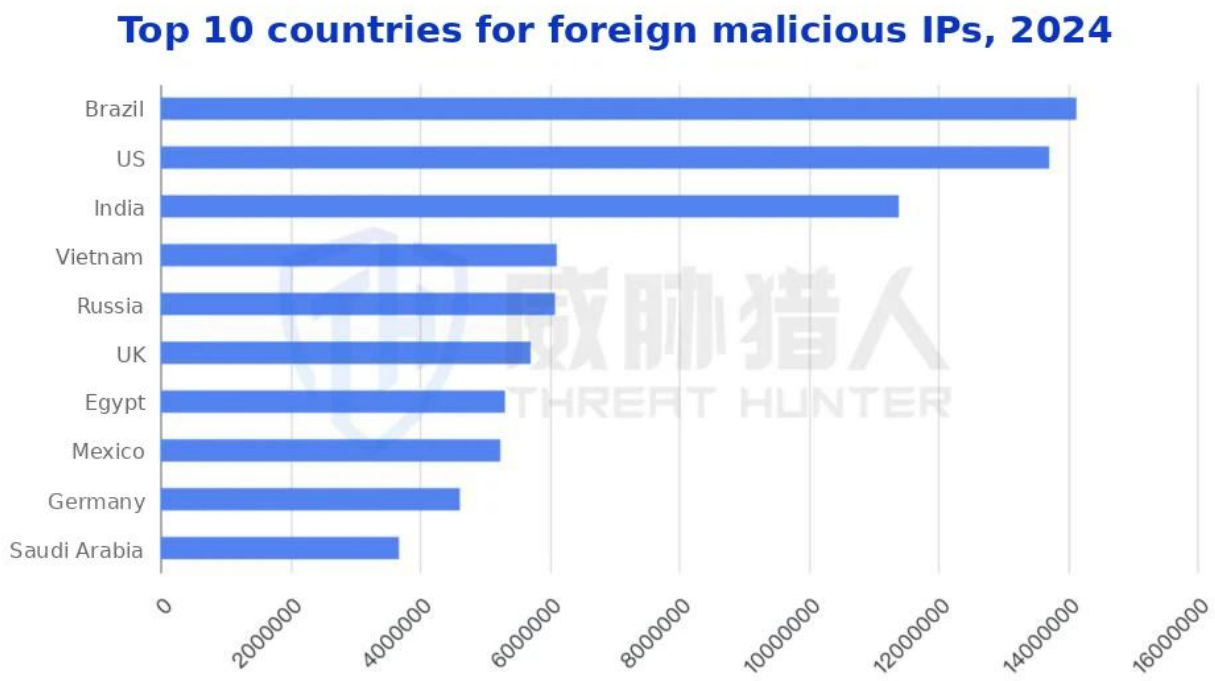
(1) In 2024, 44.79 million foreign malicious IPs were captured, an increase of 102.14% compared with 2023. In 2024, Threat Hunter strengthened the monitoring of malicious IPs outside China, and a total of 44.79 million such IPs were captured in 2024, an increase of 102.14% compared with 2023.



Foreign malicious IPs, 2023 vs 2024

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

(2) The countries where foreign malicious IPs belong to in 2024 are top 3: Brazil, the United States, and India (3) There are differences in the proportions of domestic and foreign malicious IPs types, and the proportion of foreign mobile networks far exceeds that of domestic Threat Hunter intelligence personnel analyzed the domestic and foreign malicious IPs types and found that there are differences between the two:

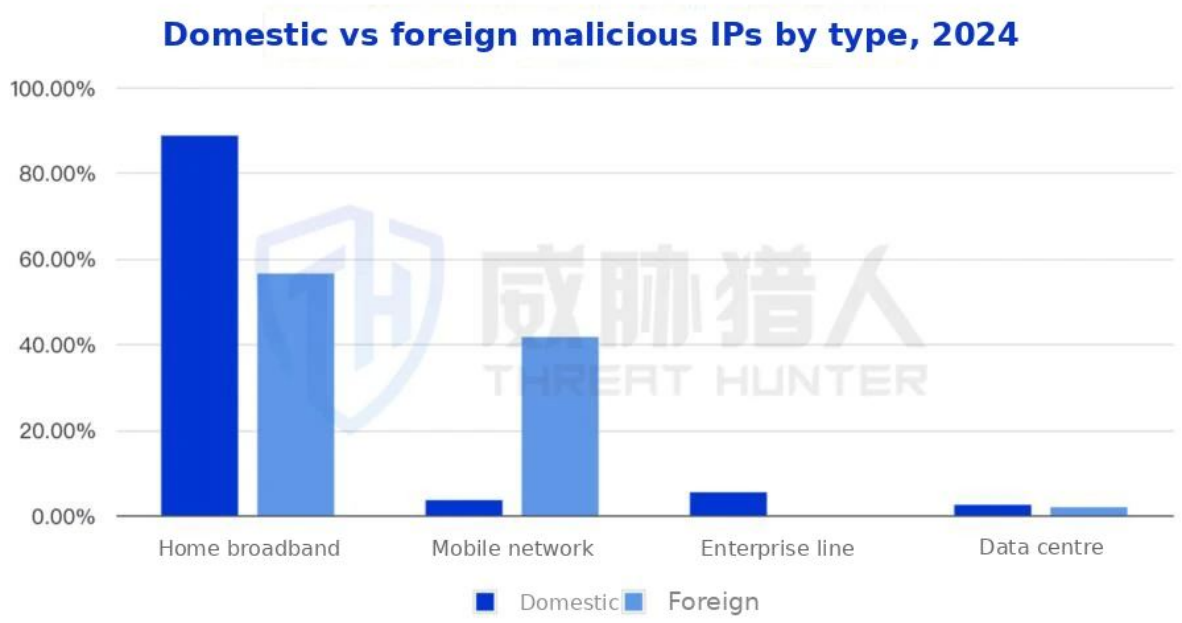


Top 10 countries for foreign malicious IPs, 2024

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

Domestic malicious IPs are mainly home broadband IPs, accounting for nearly 90%. Domestic malicious activity proxy IPs, speed dial IPs and hijacking shared proxy IPs are all closely related to home broadband;

Although foreign malicious IPs account for the largest share of household broadband, mobile networks also account for a relatively high proportion, exceeding 40%. Further analysis found that these IPs mainly come from traffic cards, and IP changes are achieved by frequently switching to airplane mode.



Domestic vs foreign malicious IPs by type, 2024

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 Analysis of bank card resources involved in money laundering in 2024

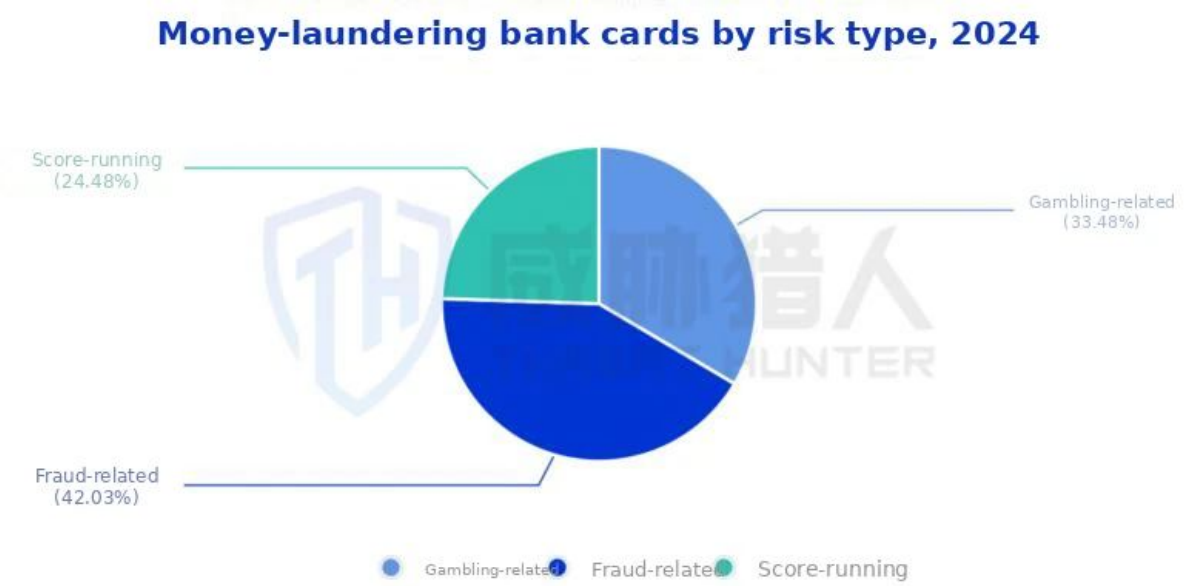
(1) Among the bank cards involved in money laundering in 2024, fraud-related cards accounted for the largest proportion, accounting for 42.03%. Threat Hunter analyzed the 336,000 bank cards captured for money laundering, which were mainly divided into three types: gambling-related cards, scorecards and fraud-related cards. Among them, fraud-related cards accounted for the largest proportion, reaching 42.03%.

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.

Benchmark card: A bank card that is active on the benchmark platform and used by scorers. It is often used for circulation transactions of funds from various illegal sources.

Threat Hunter obtains the bank card account information in the benchmark order from the benchmark platform app through an automated method.

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.

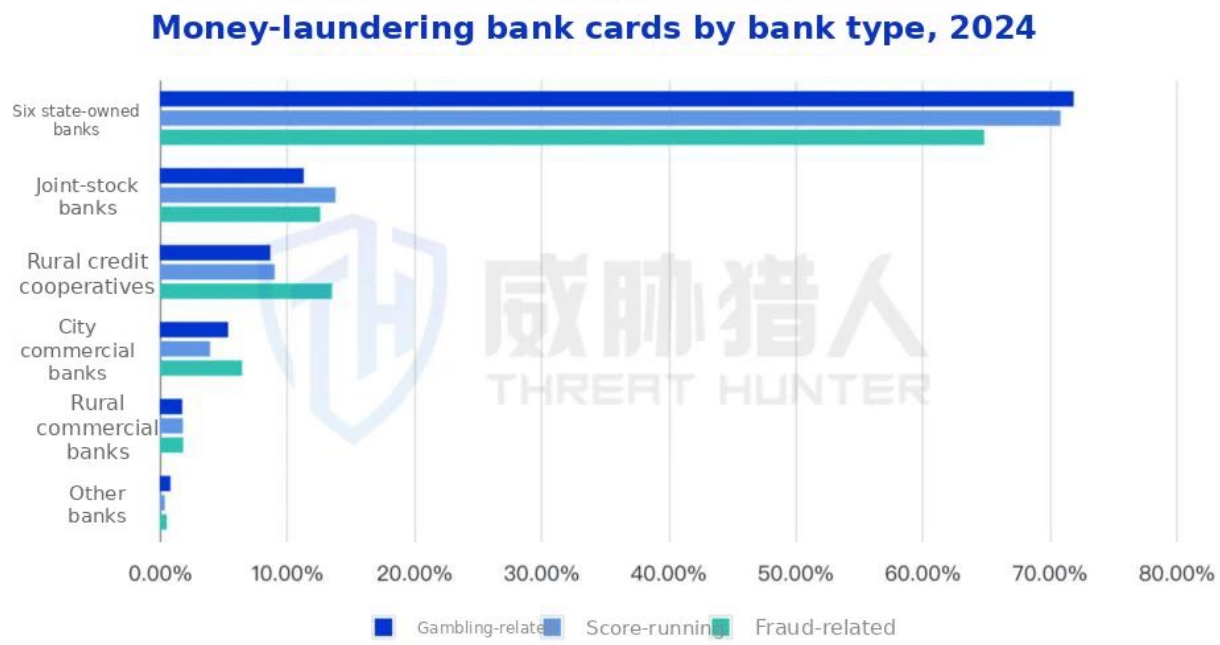


Money-laundering bank cards by risk type, 2024

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

(2) Distribution of bank cards belonging to banks involved in money laundering in 2024: The six major state-owned banks account for the highest proportion. Through monitoring data on three types of money laundering cards, Threat Hunter found that money laundering cards belonging to the six major state-owned banks account for the largest proportion. This is mainly because of its wide coverage and large customer base, making it easier for threat actors to use it as a money laundering tool. . This is mainly because of its wide coverage and large customer base, making it easier for threat actors to use it as a money laundering tool.

- Other banks include: private banks, development financial institutions and other financial institutions (3) Regional distribution of bank cards involved in money laundering in 2024: Guangdong Province has the largest number. Threat Hunter research found that there are similarities and differences in the regional distribution of the three types of money laundering bank cards:



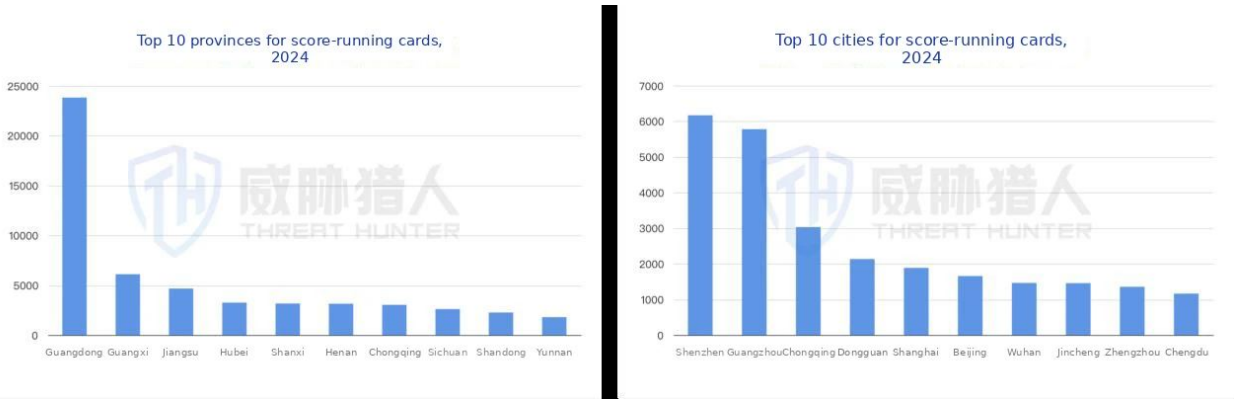
Money-laundering bank cards by bank type, 2024

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

Similarities:

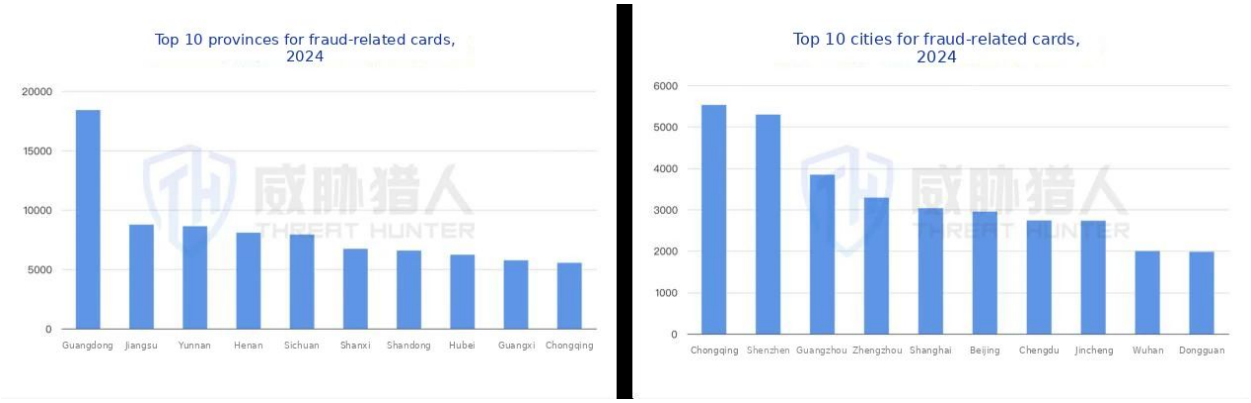
The top 10 provinces (ranked in order) for the three types of money laundering bank cards are all Guangdong, Guangxi, Jiangsu, Hubei, Shanxi, Henan, Chongqing, Sichuan, Shandong and Yunnan, and the top 1 are all Guangdong Province;

The top 10 cities (ranked in order) for the three types of money laundering bank cards are all Shenzhen, Guangzhou, Chongqing, Dongguan, Shanghai, Wuhan, Jincheng, Zhengzhou, and Chengdu; and the top 3 (ranked in order) are all Shenzhen, Guangzhou, and Chongqing.



Top 10 provinces and cities for score-running cards, 2024

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



Top 10 provinces and cities for fraud-related cards, 2024

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



Top 10 provinces and cities for gambling-related cards, 2024

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

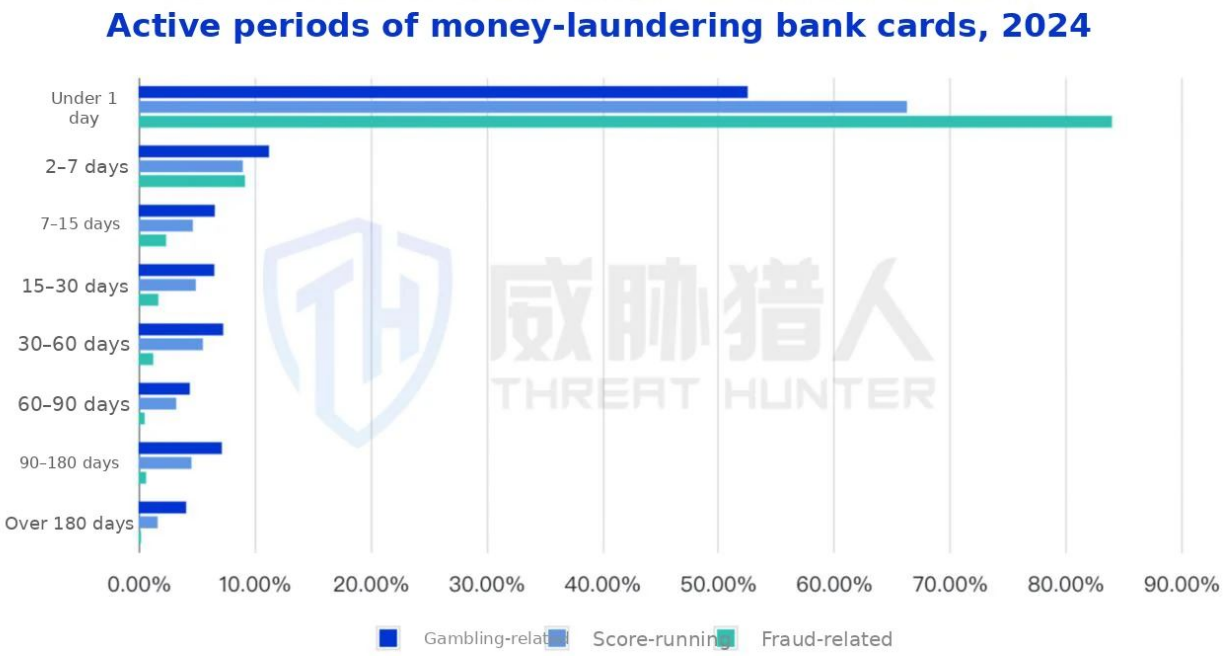
Differences:

The number of fraud-related cards in Henan, Shanxi, Sichuan, Yunnan and Shandong is higher than that of running score cards and gambling-related cards;

Chongqing has the most fraud-related and gambling-related cards, while Shenzhen and Guangzhou have the most running score cards.

(4) More than 50% of bank cards involved in money laundering have an active period of less than 1 day

Threat Hunter research found that more than 50% of bank cards involved in money laundering in 2024 were only active within one day. Among them, the proportion of fraud-related cards active within one day reached 84.03%, which was higher than 66.33% of benchmark cards and 52.58% of gambling-related cards.



Active periods of money-laundering bank cards, 2024

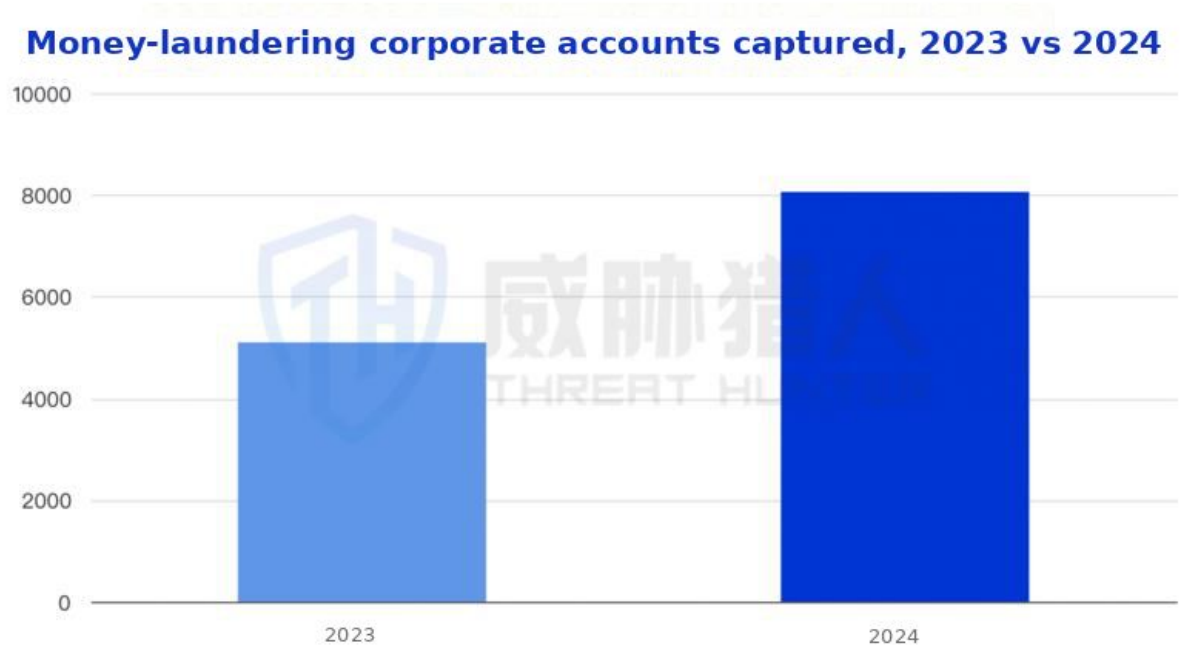
Source: Threat Hunter original report, page 25. Original figure with Chinese text replaced by English.

This also shows that in money laundering scenarios, threat actors are more inclined to complete transactions quickly and have obvious short-term and high-frequency operation characteristics, especially in fraud and money laundering scenarios.

1.3.2 Analysis of changes in corporate money laundering account resources in 2024

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 2024, there were 8,059 new public accounts involved in money laundering, an increase of 58.05% from 2023. In 2024, Threat Hunter continued to monitor the bank account resources used by threat actors in the money laundering process. According to Threat Hunter intelligence monitoring of money laundering public account data, the number of new public accounts for money laundering increased significantly in 2024, an increase of 58.05% compared with 2023.

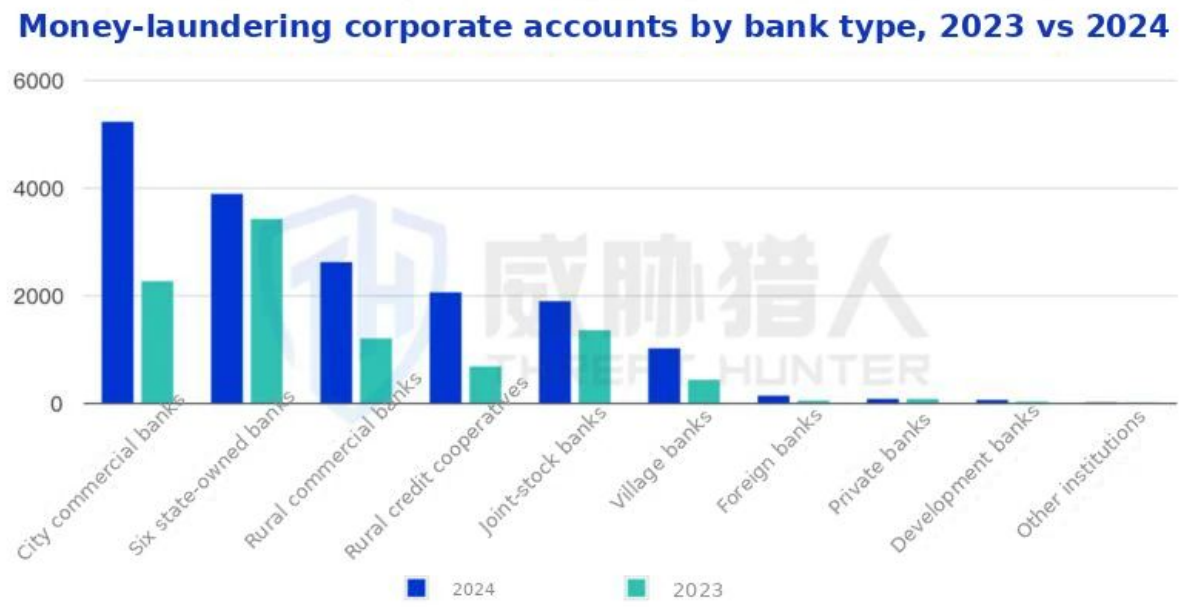


Money-laundering corporate accounts captured, 2023 vs 2024

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

(2) Among the banks with corporate accounts involved in money laundering in 2024, city commercial banks ranked first. Threat Hunter intelligence data shows that among the types of banks owned by corporate accounts involved in money laundering, city commercial banks ranked first, accounting for 30.63%.

Further analysis found that the number of corporate accounts of city commercial banks this year increased by 8.13% compared with 2023, and the number of corporate accounts of rural credit cooperatives and rural commercial banks increased by 5.48% and 3.48% respectively compared with 2023, while the proportion of the six major state-owned enterprises decreased by 11.21%.

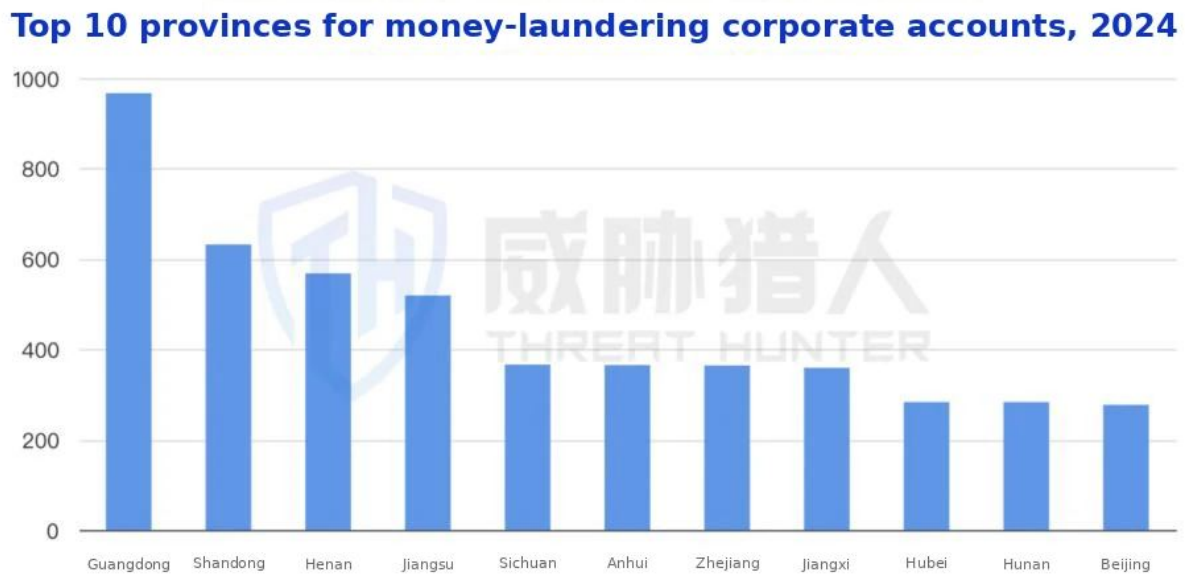


Money-laundering corporate accounts by bank type, 2023 vs 2024

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

Following this trend, threat actors may begin to turn to local banks in the process of laundering money using public accounts, and Threat Hunter will continue to pay attention.

(3) The provinces to which corporate accounts involving money laundering belong in 2024: Guangdong Province, Shandong Province, and Henan Province



Top 10 provinces for money-laundering corporate accounts, 2024

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

(4) In 2024, the three cities with the largest number of public accounts involved in money laundering were monitored: Beijing, Shenzhen, and Shanghai



Top 10 cities for money-laundering corporate accounts, 2024

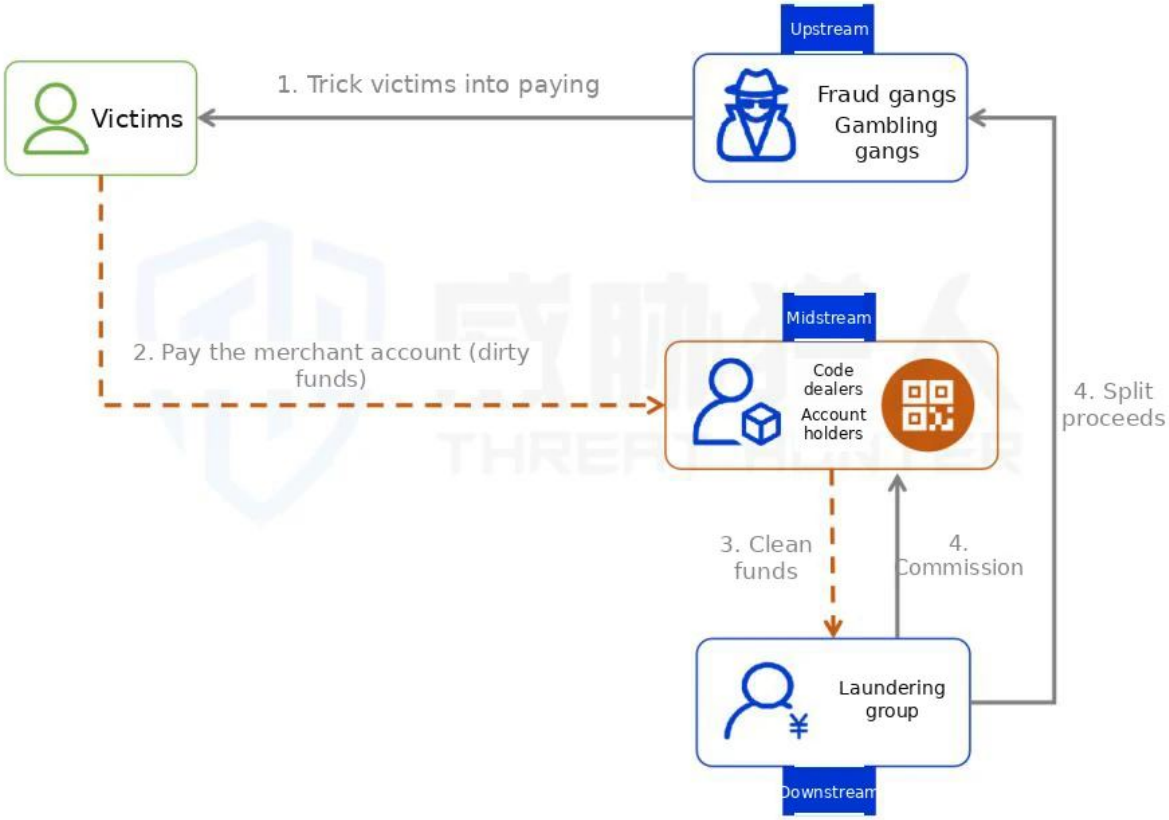
Source: Threat Hunter original report, page 27. Original figure with Chinese text replaced by English.

1.3.3 Analysis of changes in merchant resources involved in money laundering in 2024

Threat Hunter research found that in addition to using personal bank cards and public accounts to launder money, money laundering gangs also use "merchant account numbers" to launder money.

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

Threat Hunter conducted focused research on the "merchant money laundering" industry chain in 2024 and found that there have been various merchant money laundering methods such as "merchant collection" (merchant code), "street scanning code", "merchant anti-scanning", and "merchant payment" (write-off code).

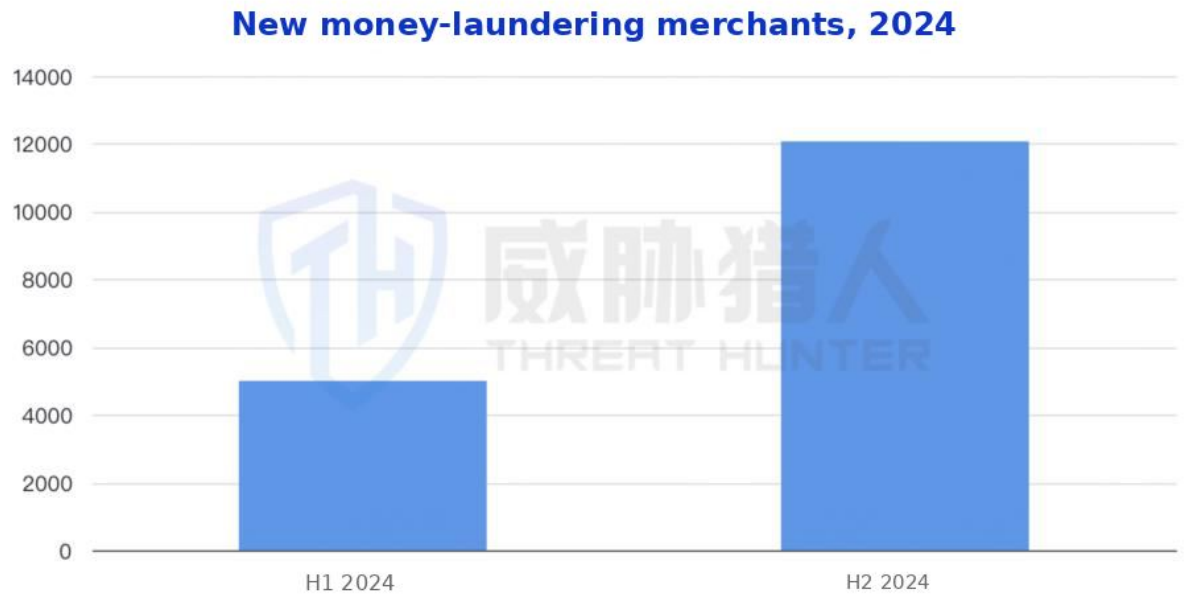


How fraud and gambling gangs launder money through merchants

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

(1) "Merchant money laundering" has become an upward trend. The number of merchants and threat actors participating in money laundering will continue to increase in 2024. Threat Hunter intelligence data shows that the number of merchants participating in money laundering will continue to increase in 2024, with an increase in the second half compared to the first half.

141.42%.



New money-laundering merchants, H1 vs H2 2024

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

In the second half of 2024, the number of active money laundering threat actor groups increased significantly, with a year-on-year increase of 81.91% in the first half of the year.



Active groups laundering money through merchants, H1 vs H2 2024

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

(2) The top three provinces where merchants involved in money laundering are located in 2024: Guangdong Province, Zhejiang Province, Sichuan Province (3) The top three cities where merchants are involved in money laundering are located in 2024: Shenzhen City, Chengdu City, Guangzhou City



Top 10 provinces for money-laundering merchants, 2024

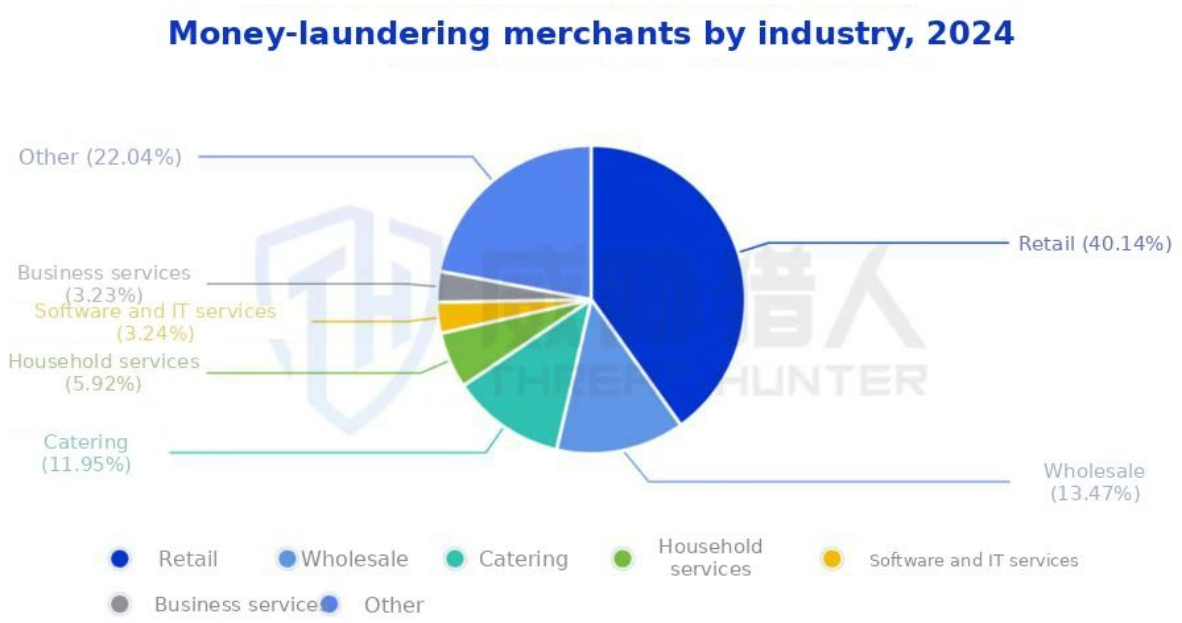
Source: Threat Hunter original report, page 29. Original figure with Chinese text replaced by English.



Top 10 cities for money-laundering merchants, 2024

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

(4) Industry distribution of merchants involved in money laundering in 2024 top 3: retail, wholesale, and catering industries Threat Hunter intelligence personnel further analyzed the merchants involved in money laundering and found that these merchants involve more than 80 industries, of which retail merchants account for the largest proportion, exceeding 40%, followed by the wholesale industry and catering industry. This type of industry has the characteristics of high frequency of capital flow, many transaction objects, and fast fund settlement. These characteristics are in line with the requirements of threat actors for money laundering. It is less likely for threat actors to use such merchants to launder money and trigger fraud controls.

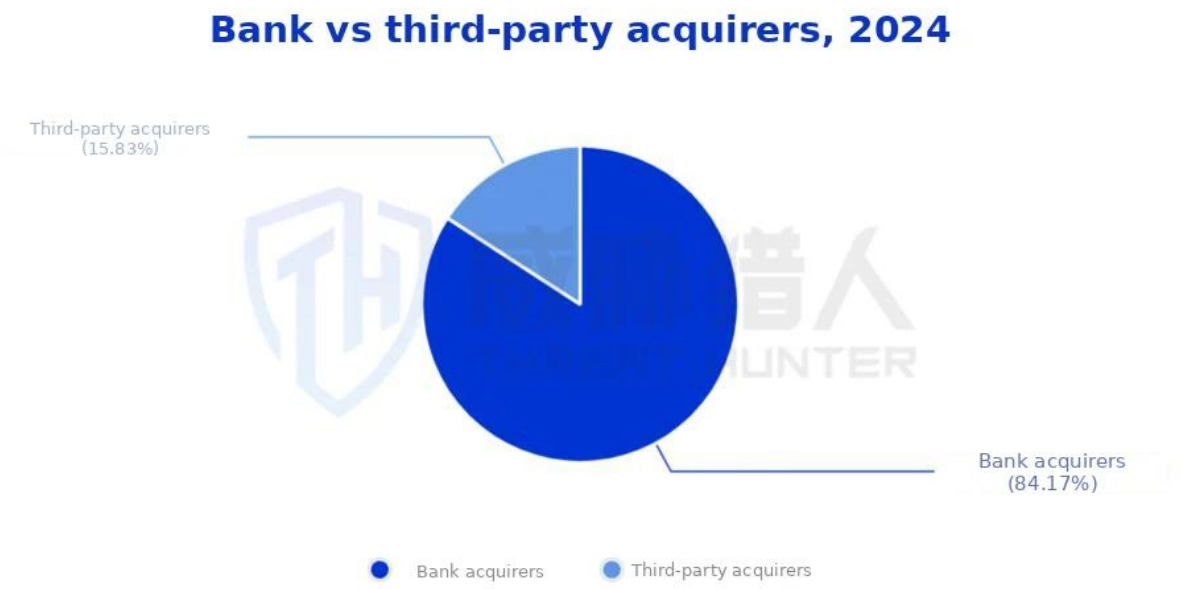


Money-laundering merchants by industry, 2024

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

(5) [Attention] 2024 Financial Industry Acquirer Money Laundering Risk Ranking Threat Hunter research found that in the "merchant money laundering" industry chain, there is a core role - the acquirer. Acquirers include both corporate third-party acquirers and banks themselves as acquirers.

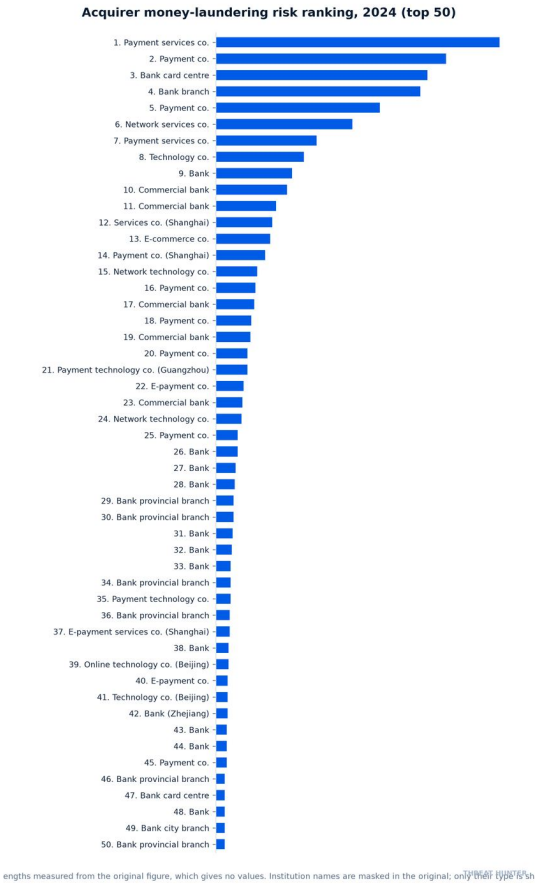
Among the more than 300 acquirers monitored by Threat Hunter that are involved in merchants' money laundering risks, banks themselves account for the largest proportion of acquirers, reaching 84.17%.



Bank vs third-party acquirers among money-laundering merchants, 2024

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

Threat Hunter ranks the top 50 acquirers involved in money laundering in 2024 based on the number of money laundering transactions:

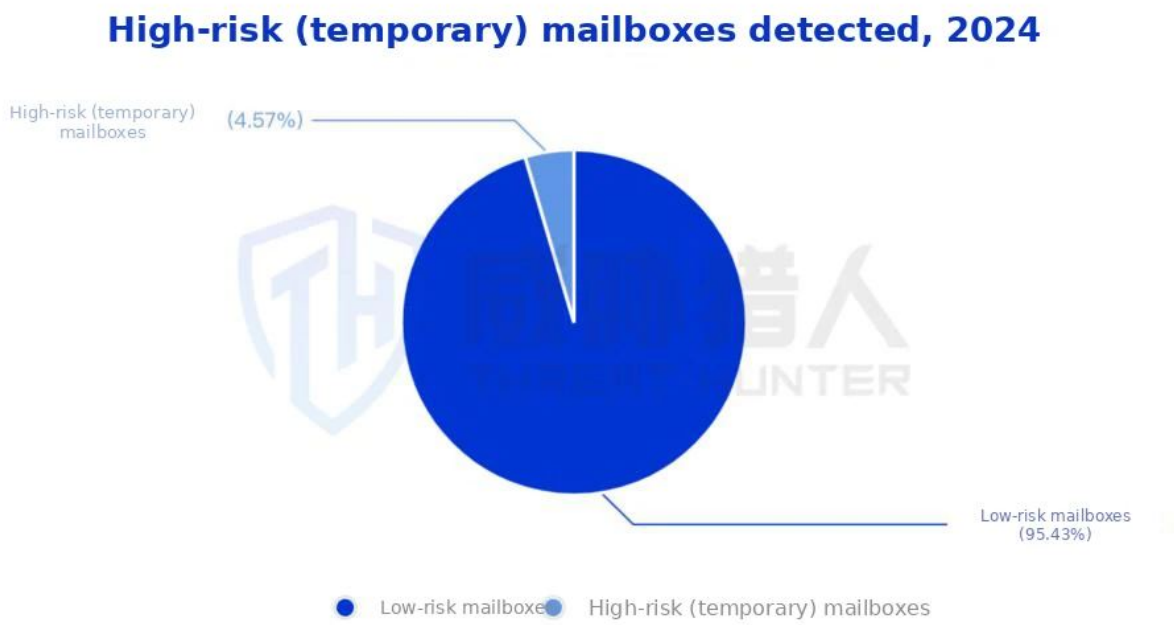


Acquirer money-laundering risk ranking, 2024

Source: Threat Hunter original report, page 31. Redrawn in English from the original figure.

1.4 Risk Email Resource Analysis in 2024

In 2024, the number of high-risk email (temporary email) domain names captured was 9,334, accounting for 4.57% of the total.

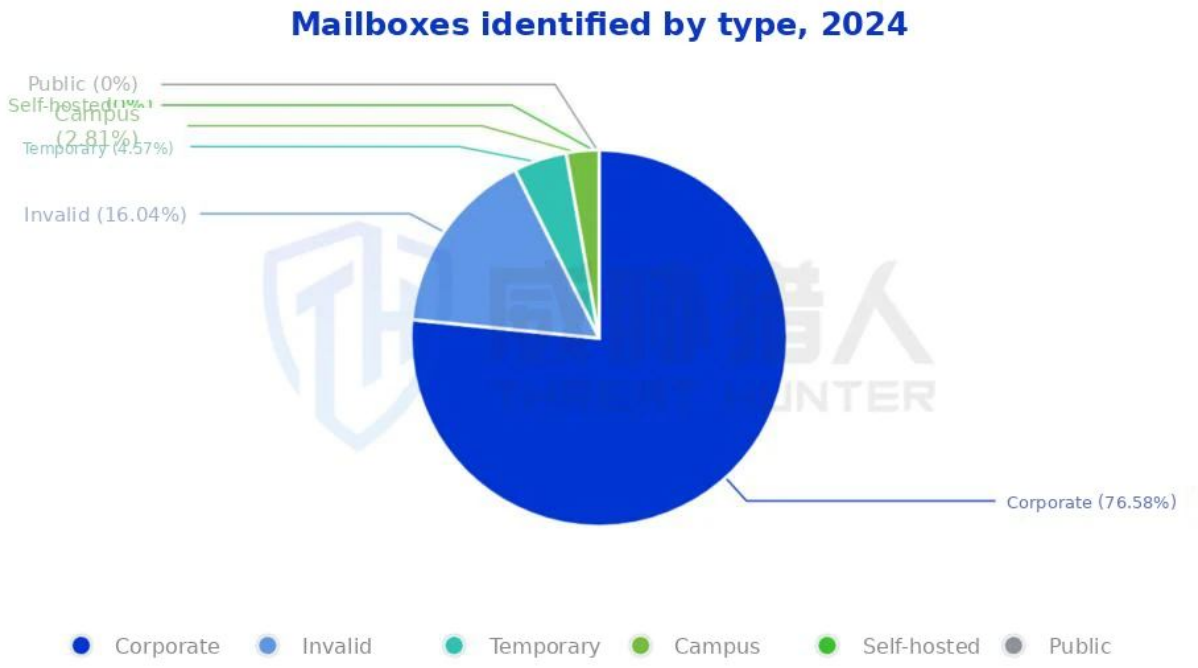


High-risk (temporary) mailboxes detected, 2024

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

Judging from the number of different types of mailboxes in 2024, 204,100 mailboxes were captured in 2024, of which low-risk enterprise mailboxes accounted for the total

76.58%, high-risk mailboxes (temporary mailboxes) account for 4.57%, and the new mailboxes this year are mainly corporate mailboxes.



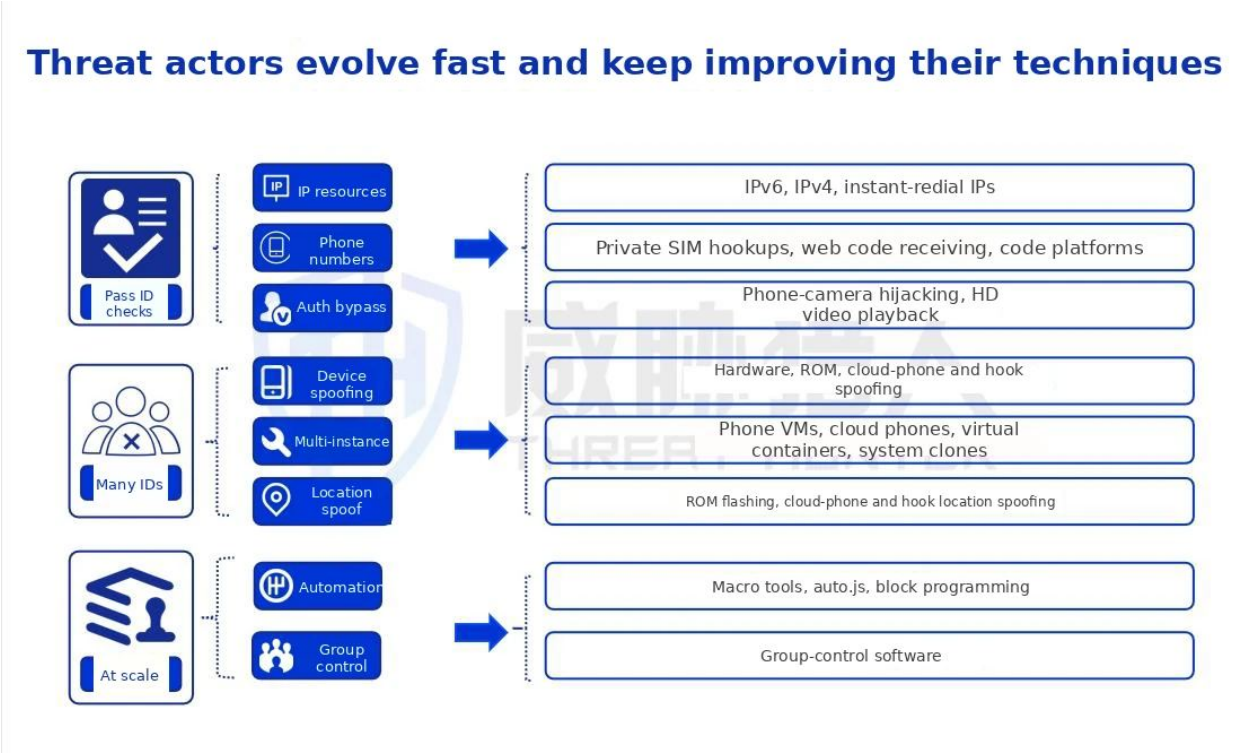
Mailboxes identified by type, 2024

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

Analysis of common cybercriminal groups attack technologies on the Internet in 2024

2. Analysis of common cybercriminal groups attack technologies on the Internet in 2024

Threat Hunter research found that since each enterprise has different business environments and fraud-control measures, the malicious tools and attack services used by threat actors against these enterprises are also diverse. However, through in-depth analysis of the underlying technical characteristics of these tools, we can divide the attack services into three major modules: "over-identity", "multi-identity" and "batch". Each of these modules involves a variety of underlying attack technologies, and these technologies are the key to realizing various specific attack behaviors.



Threat actors evolve fast and keep improving their techniques

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

2.1 Evolution of identity bypass technology: threat actors use "sub-master machines" to bypass authentication, and unqualified personnel can also take orders on the platform

Threat Hunter research found that in 2024, cybercriminal groups will use "sub-machine" technology to enable two mobile phones to log in to the same platform account at the same time. Using this technology, threat actors can enable two people to share a platform account at the same time to complete platform-related operations.

The application logic of "child-mother machine" is: threat actors first use the parent mobile phone to log in to the account to complete the identity authentication, then obtain the account's cookies, device environment and other information through code hijacking, then copy this information to the child device, replace its original file, and let the child device read the new information.



Master phone and child phone showing the same driver account

Source: Threat Hunter original report, page 35. Original figure with Chinese text replaced by English.

At present, the sale of such tools has appeared in industries such as travel and food delivery, which may lead to untrained or unqualified drivers/delivery workers working in violation of regulations, which not only affects the service quality of the platform, but may also endanger the personal safety of platform users, causing greater losses and reputational damage to the platform.

[Example of travel platform “sub-machine”] Take an app in the travel industry as an example:

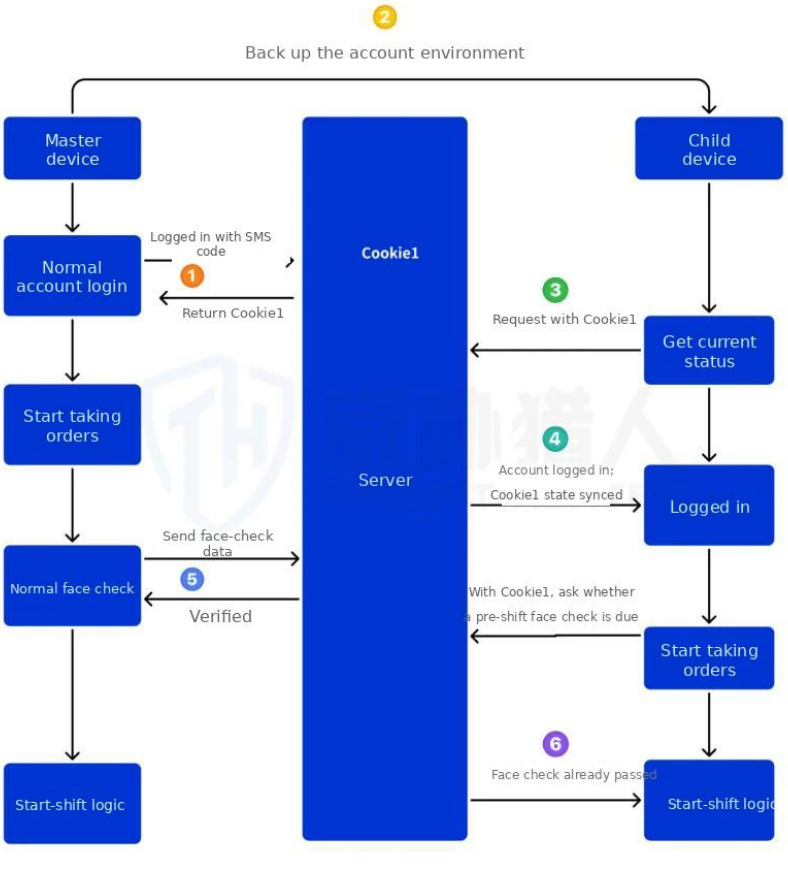
1 First, log in and authenticate Master A’s platform account on mobile phone A;

2 Then, copy the cookies and device environment information on mobile phone A to mobile phone B through hijacking and other methods;

3. B’s mobile phone is currently controlled by Master B, but the information on B’s mobile phone is Master A’s account information;

4 Each time face authentication is performed, you only need to authenticate on mobile phone A, and it will be effective on both mobile phones. Masters A and B can continue to use their accounts for business operations.

The specific process is as follows:



How the master–child phone setup passes the pre-shift face check

Source: Threat Hunter original report, page 36. Original figure with Chinese text replaced by English.

2.2 threat actors use "NFC" remote transmission software to launder money across borders and move illegal funds

Threat Hunter research found that in 2024, cybercriminal groups used "NFC technology" to implement remote money laundering activities.

NFC (Near Field Communication) is a short-range wireless communication technology. The effective distance is usually within 10cm. It is widely used in mobile wallets, access control cards, data exchange and other fields.

The so-called NFC remote transmission refers to reading device information through NFC technology and then transmitting the information remotely through the network. For example, after device A reads the IC card information, it sends the information to the server or device B through a specific application, and device B can simulate the use of the IC card.

cybercriminal groups use this technology to realize remote reading and recovery of IC card information. Even if mobile phone device B is physically separated from the IC card, operations such as POS machine payment can be performed.

The most typical attack case is money laundering: threat actors remotely transmit domestic credit card information to foreign devices, and use this information to make purchases at POS machines, purchase luxury goods, jewelry, etc., thereby bypassing geographical restrictions on credit card transactions and completing money laundering.

Take a certain transmission app discovered by Threat Hunter as an example:

1 The software introduction “is not restricted by time or national boundaries, and can complete transactions anytime and anywhere”, “can be physical or virtual, and supports all wallets”:



Promotion for an NFC relay app

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

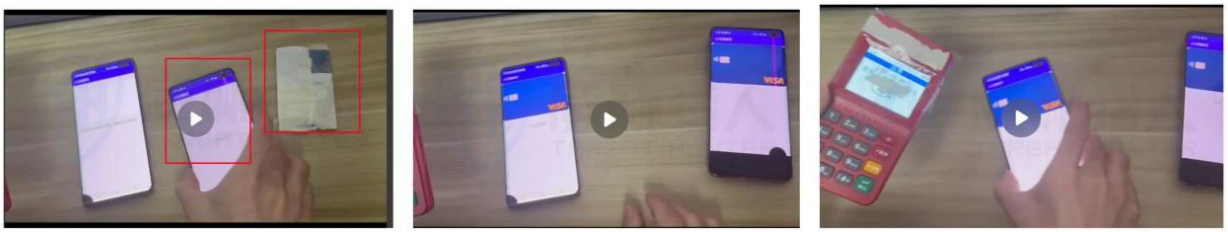
2 Download this software on both domestic (card transmitter) and foreign (receiver) mobile phones;

3. Use a domestic mobile phone to touch the physical bank card. At this time, the bank card information will be transmitted to the domestic mobile phone;

4. After the domestic mobile phone receives the bank card information, it will transmit the bank card information to the foreign mobile phone through the software installed on the mobile phone;

5. After the foreign mobile phone receives the bank card information through the software, it can swipe the card normally.

Figure A: Domestic mobile phone (card transfer party) touches the bank card. Figure B: Domestic/foreign mobile phones receive bank card information. Figure C: Foreign mobile phone makes payment. The specific process is as follows:



NFC relay in use

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



How NFC relay moves card data abroad

Source: Threat Hunter original report, page 38. Original figure with Chinese text replaced by English.

2.3 Customized cloud mobile phone system to further improve the attack efficiency of threat actors

Threat Hunter pointed out in the "Internet cybercrime ecosystem research annual report" released in 2023 that the supporting services of the cloud mobile platform are increasingly abundant, and the threat actors technology shows the characteristics of integration and service. In 2024, we will continue to follow and observe and find that the cloud mobile phone platform is not only becoming more integrated and service-oriented, but the trend of customization is also becoming more mature.

Servitization mainly provides complete basic attack tools, allowing users to carry out attacks based on these tools. Customization means that the cloud phone platform bypasses fraud controls for specific apps, develops corresponding malicious scripts, and integrates them into the cloud phone system for direct use by users.

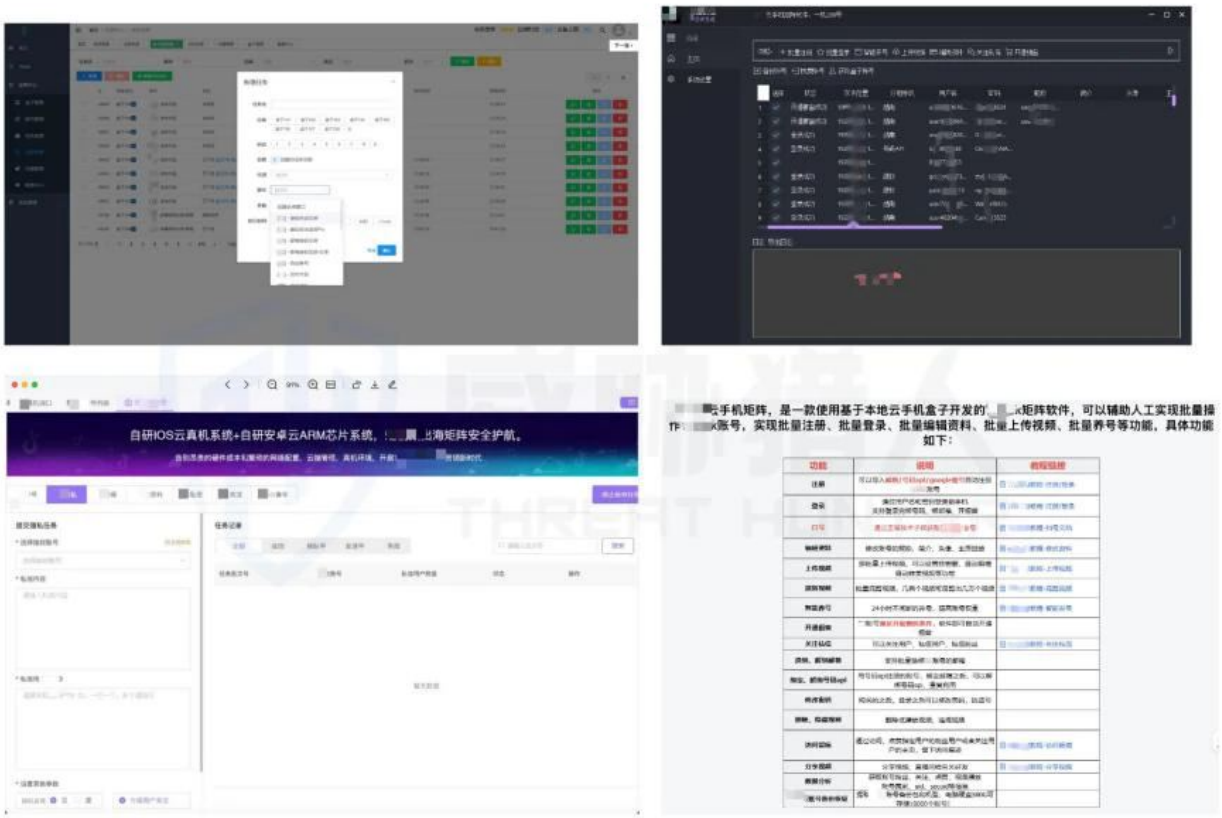


Cloud-phone platform add-ons, 2023 vs 2024

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

Take a social app as an example:

The cloud mobile phone system customized and developed by threat actors covers the automation of complete attack processes such as registration, account maintenance, and traffic monetization. This not only lowers the entry threshold for attackers, allowing novices to perform fool-like operations, but also eliminates the need for attackers to pay attention to confrontation at the fraud controls level, thus greatly improving attack efficiency.



Customized cloud-phone control system

Source: Threat Hunter original report, page 39. Original image retained.

Analysis of cybercriminal groups attack scenarios on the Internet in 2024

3. Analysis of cybercriminal groups attack scenarios on the Internet in 2024

3.1 Online business fraud scenarios

The online business fraud scenarios in this report are not limited to traditional marketing activity fraud attacks. All malicious behaviors that interfere with normal business operations and make profits from normal business development are called "business fraud attacks," such as marketing fraud, malicious traffic diversion, manipulate fraud, authentication bypass, etc.

3.1.1 The risk of online business fraud will continue to grow in 2024, with nearly 300 million related attack intelligence

In 2024, Threat Hunter captured a total of 272 million pieces of information related to business fraud attacks, monitored 120,000 business fraud groups, and involved 2.23 million malicious accounts.

In December 2024, business fraud-related intelligence increased dramatically. Threat Hunter intelligence personnel further analyzed and found that more than half of the increase in December

came from intelligence information on anonymous group chats. This phenomenon was mainly caused by the frequent online gambling activities of some large gambling threat-actor groups, and the money laundering gangs using multiple accounts to conduct advertising "recruitment" and violent diversion.



Business fraud attack intelligence by month, 2024

Source: Threat Hunter original report, page 41. Original figure with Chinese text replaced by English.

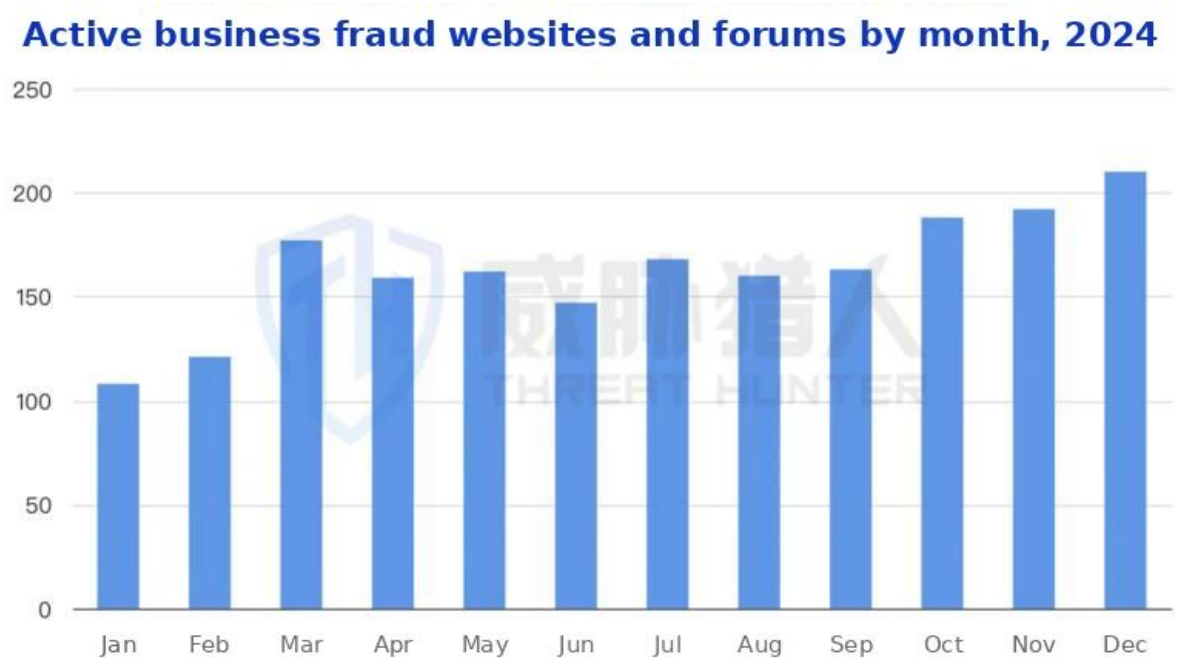
In 2024, Threat Hunter captured a monthly average of 32,000 active business fraud groups:



Active business fraud groups by month, 2024

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

In 2024, Threat Hunter captured an average of 163 active business fraud websites/forums (excluding dark web) per month, and the total number of malicious posts throughout the year was 9.26 million:



Active business fraud websites and forums by month, 2024

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

In 2024, Threat Hunter captured an average of 320,000 active business fraud accounts for several months:



Threat actors involved in business fraud by month, 2024

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

3.1.2 There were 4,158 fraud incidents in the early warning business in 2024, involving the entire industry and business

The Threat Hunter risk intelligence platform provides customers with risk intelligence mining and event warning services, supporting in-depth analysis and structuring of cybercrime ecosystem original clues into effective attack events. In 2024, the platform has alerted cooperative customers to 4,158 clear attack events, an average of approximately 346 per month.

Through further analysis of these attack incidents, we found that business fraud attacks have penetrated into multiple industries and multiple businesses. In other words, online business fraud presents "indiscriminate attacks" against different industries and different business links. Any profitable place is the target of cybercriminal attacks.



Marketing fraud events by industry, 2024

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

By extracting hot words from attack events, we found that current business fraud attacks are not limited to businesses such as registration and login, coupon collection and order grabbing in the past. Content publishing, product management, order transactions, payment transactions, after-sales payments, enterprise data transmission and other aspects may be attacked and profited by threat actors.



Hot words in business fraud attack events, 2024

Source: Threat Hunter original report, page 44. Redrawn in English from the original figure.

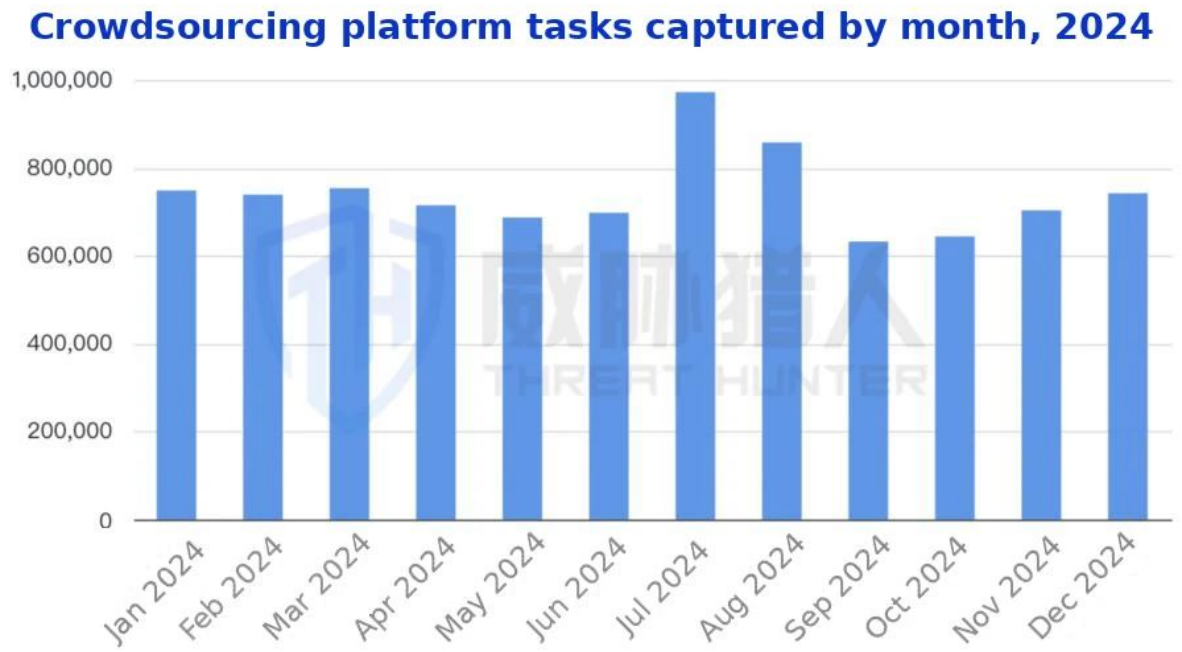
3.1.3 Business fraud has entered deep waters, human-operated fraud has become increasingly customized, and role boundaries have become more blurred.

With the continuous improvement of business fraud-control capabilities, most typical automated fraud behaviors have been effectively identified. Although some high-end threat actors still use customized technology to fight, more and more the cybercrime ecosystem actors are turning to human-in-the-loop crowdsourcing fraud methods to conduct attacks.

Judging from the intelligence information captured by Threat Hunter, in 2024, human-operated fraud became more customized, with diverse roles and blurred boundaries. Mainly reflected in the following aspects:

(1) The traditional task-based crowdsourcing platform, that is, the model based on "publishing tasks" and "receiving tasks", continues to grow in both the number of platforms and the number of tasks.

Since 2024, Threat Hunter has captured a total of 8.89 million crowdsourcing tasks, with an average of more than 630,000 per month, and even reaching 1 million during peak periods.



Crowdsourcing platform tasks captured by month, 2024

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

(2) cybercriminal groups adopt a more covert form of crowdsourcing organization, such as recruiting human participants to perform specific tasks through crowdsourcing private domain group chats and developing special apps. This model is similar to the real crowd of fake orders and is difficult to be identified by the fraud-control system. These special tasks may include disguised swiping of orders, browsing hotel pages to increase pageviews, or using accounts operated by real users to hang up and crawl platform product data, etc.

Case 1: Taking the "Hotel Screenshots" crowdsourcing project as an example, threat actors developed an app called "Zhitip xx", through which part-time workers were organized to complete the task of hotel screenshots.

Participants follow the tutorial provided by the app, intercept the price information from the hotel page and upload it for the designated check-in platform, date, region and hotel name. The app will automatically identify and extract price information through OCR technology, and participants can then receive the corresponding commission.



Crowdsourcing app for the hotel screenshot project

Source: Threat Hunter original report, page 46. Original image retained.

Case 2: cybercrime ecosystem creates a group in the name of part-time job, organizes and recruits human participants to use their accounts to access product links on designated e-commerce platforms, and obtains the corresponding number of products and the price of the corresponding activity conditions to upload the form as required. This is a kind of "human crawler" behavior.

序号	商品ID	商品链接	最大购买件数	1件到手价	2件到手价	3件到手价	备注	是否百亿补贴	1件到手价截图	姓名
12501	1006418	https://item 0703.ht	2	89.1	178.2			否		朱
12502	1009976	https://item 9272.ht	1	158				否		朱
12503	1008938	https://item 1043.ht	2	139	278			否		朱
12504	1000144	https://item 17.html	3	84	168	214.2		否		朱
12505	1006102	https://item 4008.ht	1	79				否		朱
12506	1003972	https://item 7866.ht	2	89.1	178.2			否		朱
12507	1003650	https://item 0260.ht	1	169				否		朱
12508	1010301	https://item 0917.ht	2	610.8			无货	否		朱
12509	1004096	https://item 1158.ht	1	149				否		朱
12510	1000483	https://item 89.html	1	139				否		朱
12511	1008800	https://item 9279.ht	2				下架且无价	否		朱
12512	1000961	https://item 97.html	2	89	178			否		朱

Recruiting human participants through part-time job groups

Source: Threat Hunter original report, page 46. Original image retained.

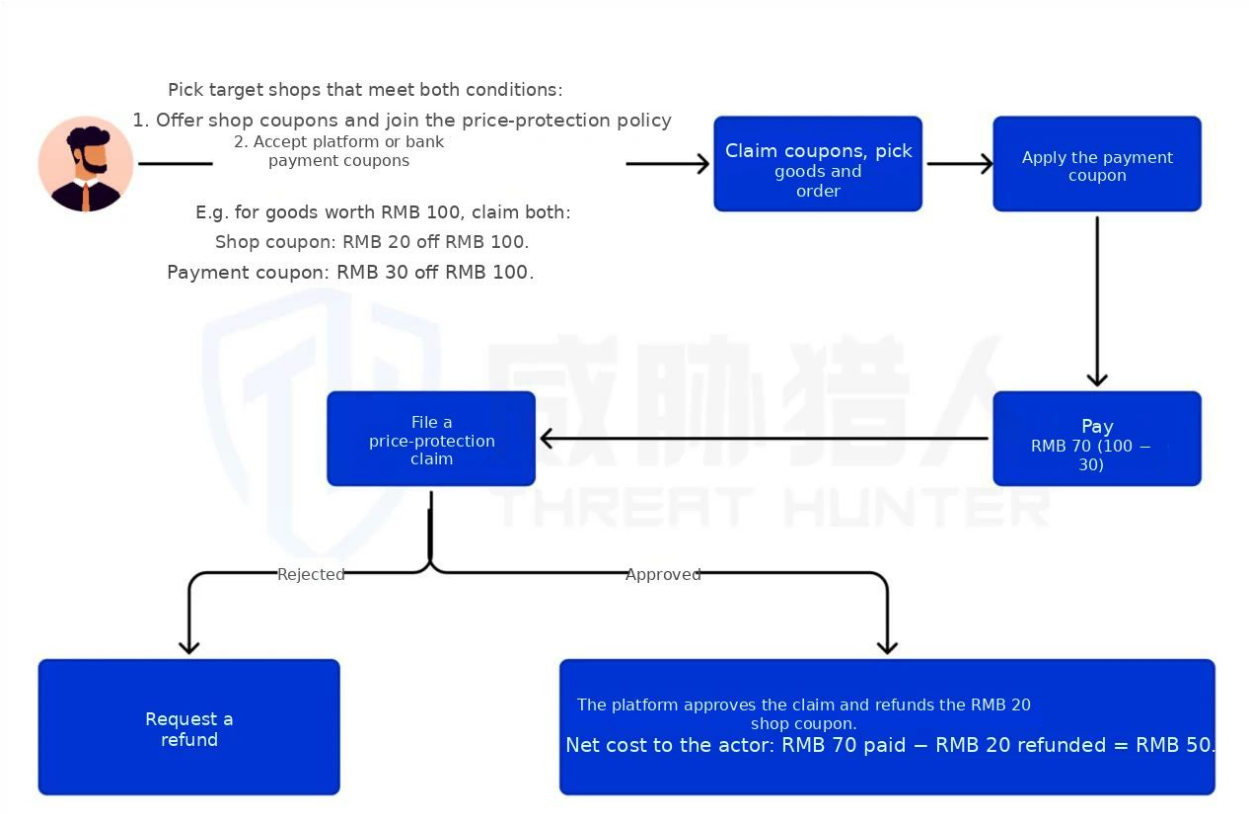
(3) The boundaries of fraudulent roles are gradually blurring, and more and more real users are making malicious profits by studying and using the "legitimate" rules of platform business.

In recent years, multiple platforms have emerged one after another with multiple compensation, refund-only tutorials, and price guarantee refund strategies, which more reflect the trend of fraud led by real users of the platform under the "guidance" of the cybercrime ecosystem.

Case: Threat Hunter captured a promotion-abuse actor who used the platform's price guarantee policy combined with payment coupon identification loopholes to purchase platform products "for zero" or at a low price. This type of attack caused large losses and refunds to the platform and merchants who had opened the price guarantee in a short period of time.

The promotion-abuse actors found that a certain type of product on a certain platform can receive full discount coupons and payment coupons (cooperative bank or platform category), but they can only choose to use one of the two; the promotion-abuse actors purchased the product through a payment coupon, and then used the merchant's price guarantee policy rules to apply for a store to fully discount the guaranteed price of the coupon (the merchant cannot see that the user used the payment coupon because it is a different platform), and finally reached 0% or purchased at a low price.

Threat Hunter intelligence personnel analyzed this type of vulnerability attack and found that promotion-abuse groups mainly exploited vulnerabilities in two aspects: first, they took advantage of the compensation mechanism for store coupons in the price guarantee policy, which was originally intended to compensate users in a short period of time;



How actors stack coupons and abuse price protection

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

Secondly, they took advantage of the loophole in the price guarantee policy's inability to identify the coupon discounts that have been used. This allows threat actors to "enjoy" the benefits of both coupons at the same time. This behavior caused large losses and refunds to the platform and merchants who had opened the price guarantee in a short period of time.

3.1.4 The threat actors trading market is more active, with an average of 1.01 million goods sold per month, involving membership rights, tutorial tools, and underground services.

The continuous and efficient operation of the cybercrime ecosystem chain is inseparable from upstream resource transactions and downstream arbitrage realization. Upstream threat actors purchase attack resources such as accounts, tools, and phone numbers through specific channels. Downstream threat actors use various channels (card issuing websites and second-hand idle trading platforms, etc.) to monetize the upstream attack resources they hold as well as coupons, cash coupons, membership rights, physical goods, etc. obtained from attacks.

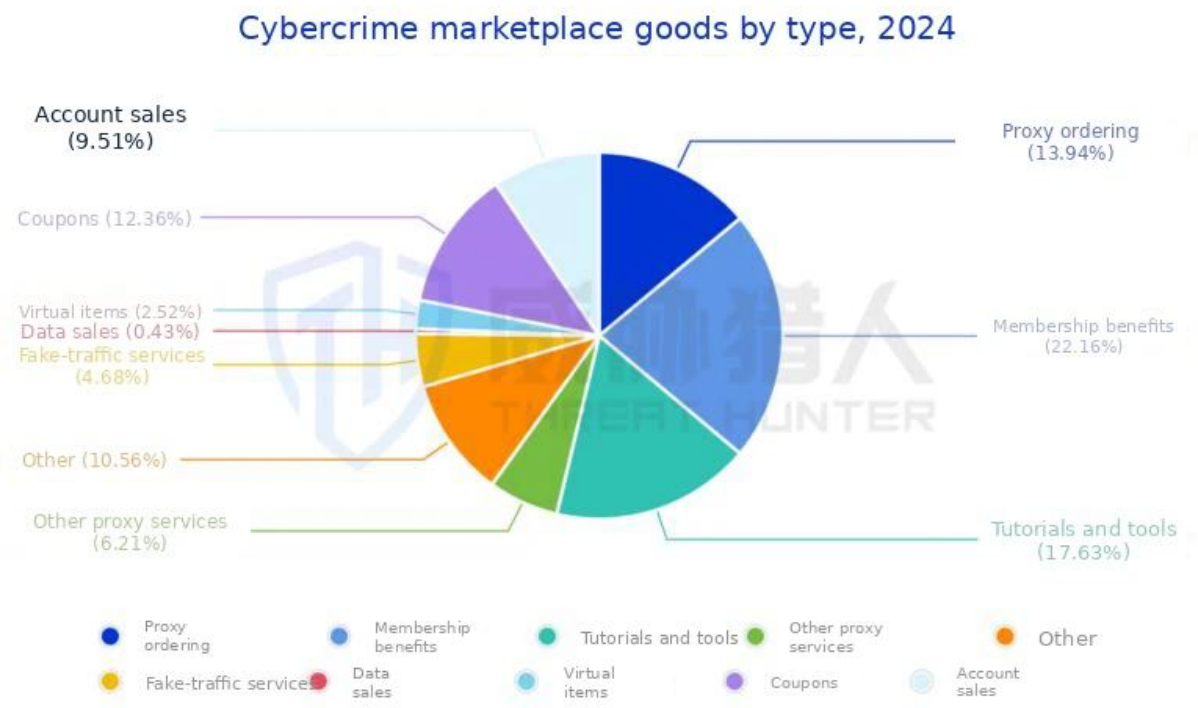
Since the cybercrime ecosystem trading market was officially launched in July 2024, a total of 6.1 million cybercrime ecosystem trading products have been captured, with an average of 1.01 million per month. The large number of actively traded products and rich categories indicate that cybercriminal attack activity are still on the rise and continue to operate. The flow of the commodity trading market actually destroys the equal rights and interests of platform users and players, and reduces and damages the expected profits of the business side.



Goods listed on cybercrime marketplaces by month, Jul–Dec 2024

Source: Threat Hunter original report, page 48. Original figure with Chinese text replaced by English.

Based on cybercrime ecosystem transaction product data captured since July, the most popular product categories are: membership rights, tutorial tools, and agent ordering service types, accounting for 22.16%, 17.63%, and 13.94% of the total transaction volume respectively.



Cybercrime marketplace goods by type, 2024

Source: Threat Hunter original report, page 48. Original figure with Chinese text replaced by English.

There are multiple subdivisions and rich products under each major product category. For example, the membership rights category includes member resale, level and joint rights of cooperative platforms. VIP rights and interests; the coupon category includes platform red envelopes, coupons, and resale of discount coupons; the tutorial tool category includes all-in-one machines, bypassing face verification, changing positioning, snapping up, order grabbing and other automation, batch fraud tools, brick-moving project tutorials, etc.; the ordering service type includes collecting usage fees, using the business party's discount account, membership rights, and subsidy quotas to place and grab orders on behalf of others; the agency service type is related to agency registration and qualification bypass, and a large number of products have violated regulations.

Tutorial tool products: online car hailing machines, targeted at fraud drivers whose qualifications have not passed the review and who want to take orders with multiple accounts to increase their income.



Advert for an online car-hailing tool

Source: Threat Hunter original report, page 49. Original image retained.

Agent service products: illegal bypass services, such as using information gaps and internal channels to directly operate on the platform for merchants, stores, drivers, etc. who apply for non-compliant qualifications.



Advert for an illegal bypass service

Source: Threat Hunter original report, page 49. Original image retained.

Agent ordering service products: various low-priced card coupons and self-service ordering products. Through the agent service and the self-service docking and ordering system built upstream, threat actors sell the recovered coupons for arbitrage, and the promotion-abuse actors obtains the goods at a lower price than the original price.



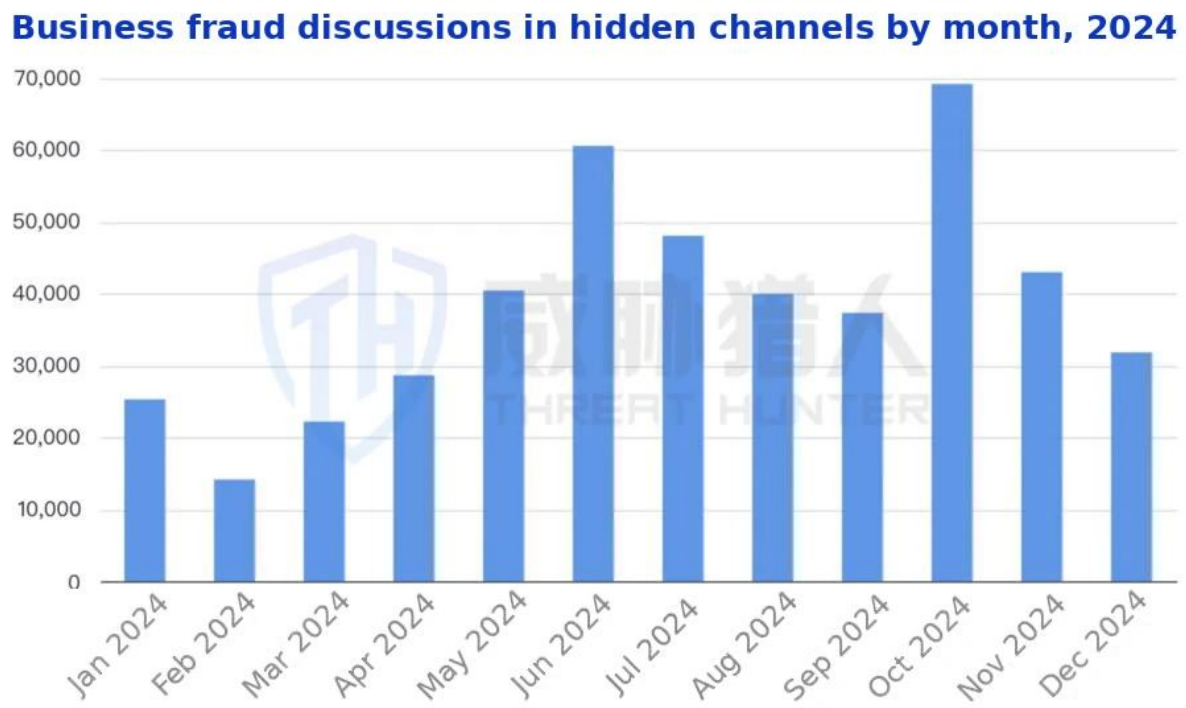
Advert for low-priced proxy ordering

Source: Threat Hunter original report, page 50. Original image retained.

3.1.5 Business fraud attacks by threat actors gradually move to more secretive channels, making monitoring more difficult.

Threat Hunter noticed that compared with the past when they mainly posted on ordinary social platforms, more business fraud threat actors are now gradually turning to more secretive channels, such as establishing a large number of business fraud-related discussion channels in anonymous group chats on encrypted messaging apps.

In 2024, Threat Hunter monitored that the number of discussions surrounding business fraud risks reached 460,000 on anonymous channels, and is showing a growing trend every month.



Business fraud discussions in hidden channels by month, 2024

Source: Threat Hunter original report, page 50. Original figure with Chinese text replaced by English.



Hidden-channel groups discussing business fraud by month, 2024

Source: Threat Hunter original report, page 51. Original figure with Chinese text replaced by English.

Learn more about the information released by active channels in anonymous channels. The information involves activity scripts that attack business activities, promotion-abuse discussions, malicious compensation tutorials, order grabbing tools, etc. The second half of the year increased by 91.43% compared with the first half of the year.

The cases involved include but are not limited to anti-counterfeiting projects, automatic collection of events, and travel industry order grabbing tools. Trading channel:



Project list posted in a hidden channel

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

3.2 Financial loan fraud scenario

Threat Hunter research found that financial loan fraud has formed a mature industry chain with clear division of labor and divided interests. Taking "professional debt" as an example, its upstream operators, intermediate threat actors, downstream intermediaries, debtors and other roles each perform their own duties and organize fraudulent loan activities through a strict collaboration mechanism. The existence of such threat actors not only disrupts the normal operation of financial markets and causes huge losses to financial institutions, but also poses a serious threat to social stability and healthy economic development.

3.2.1 The risk of loan fraud remained severe in 2024, and the popularity of fraud continues to rise

In 2024, Threat Hunter captured a total of 4.14 million pieces of loan fraud attack intelligence, monitored 34,697 active malicious activity social groups, and 115,000 malicious activity threat actors; whether it is the popularity of fraud intelligence, the number of malicious activity groups, or the number of malicious activity threat actors (including malicious loan intermediaries), there is a gradual upward trend.

(1) In 2024, 4.14 million pieces of malicious loan fraud intelligence were captured, which continued to increase every month. (2) In 2024, 34,697 active malicious social groups were monitored, an increase of 30% in the second half of the year compared with the first half.



Loan fraud intelligence by month, 2024

Source: Threat Hunter original report, page 52. Original figure with Chinese text replaced by English.



Active loan fraud groups by month, 2024

Source: Threat Hunter original report, page 52. Original figure with Chinese text replaced by English.

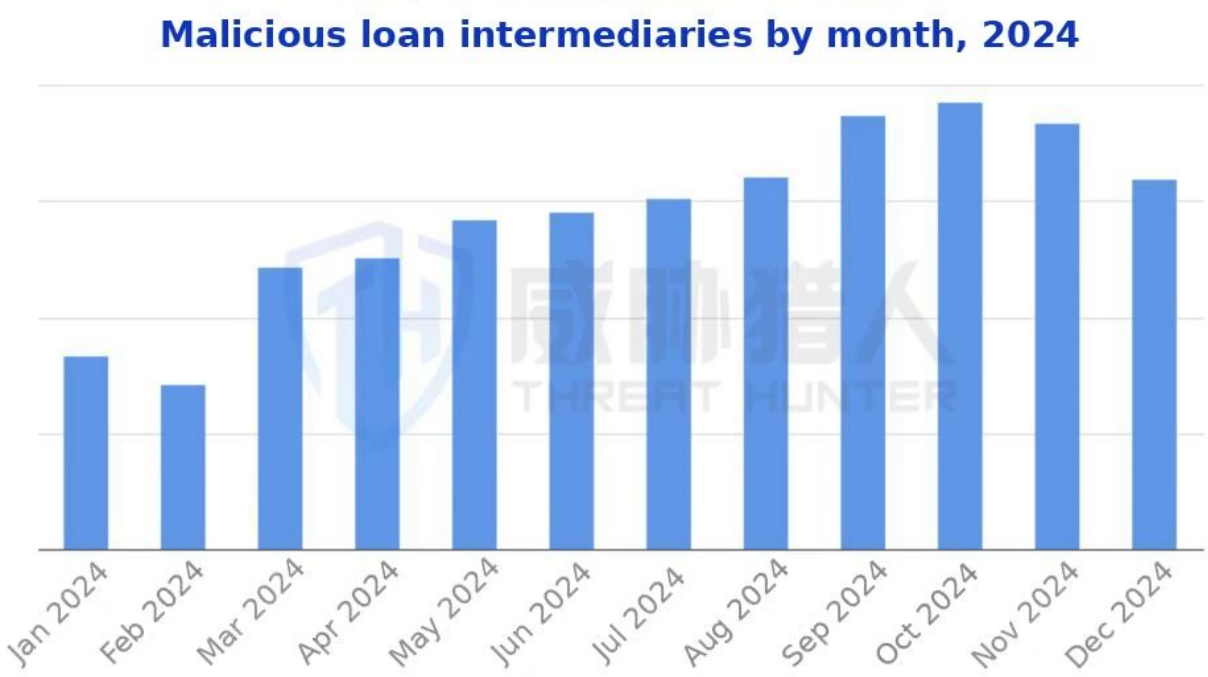
(3) In 2024, 115,000 threat actors committing loan fraud were captured, and the number of threat actors conducting malicious activity in the second half of the year increased by 51% compared with the first half of the year.



Threat actors committing loan fraud by month, 2024

Source: Threat Hunter original report, page 53. Original figure with Chinese text replaced by English.

(4) There were 43,000 malicious loan fraud intermediaries in 2024, and the number of malicious loan intermediaries in the second half of the year increased by 50% compared with the first half of the year.

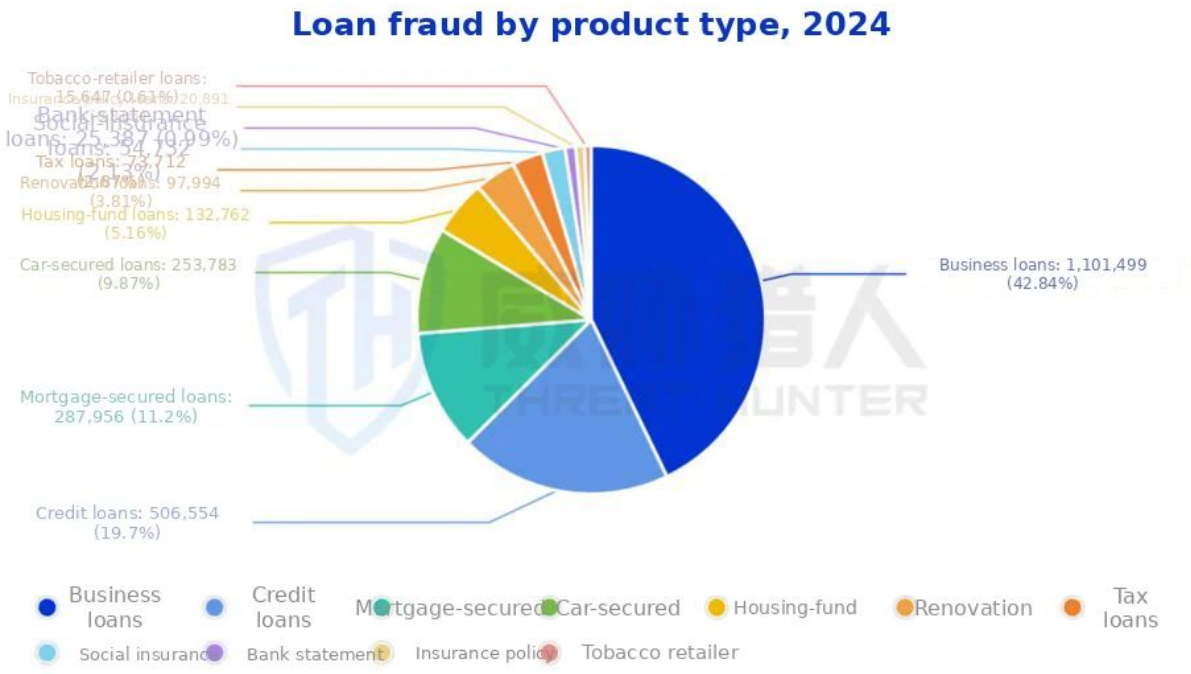


Malicious loan intermediaries by month, 2024

Source: Threat Hunter original report, page 53. Original figure with Chinese text replaced by English.

3.2.2 Popularity of loan fraud product types in 2024 top 3: corporate loans, credit loans, housing mortgage loans

From the perspective of loan product types, the top five loan product types with the most popular credit fraud in 2024 are: corporate loans, credit loans, housing mortgage loans, car mortgage loans, and provident fund loans.

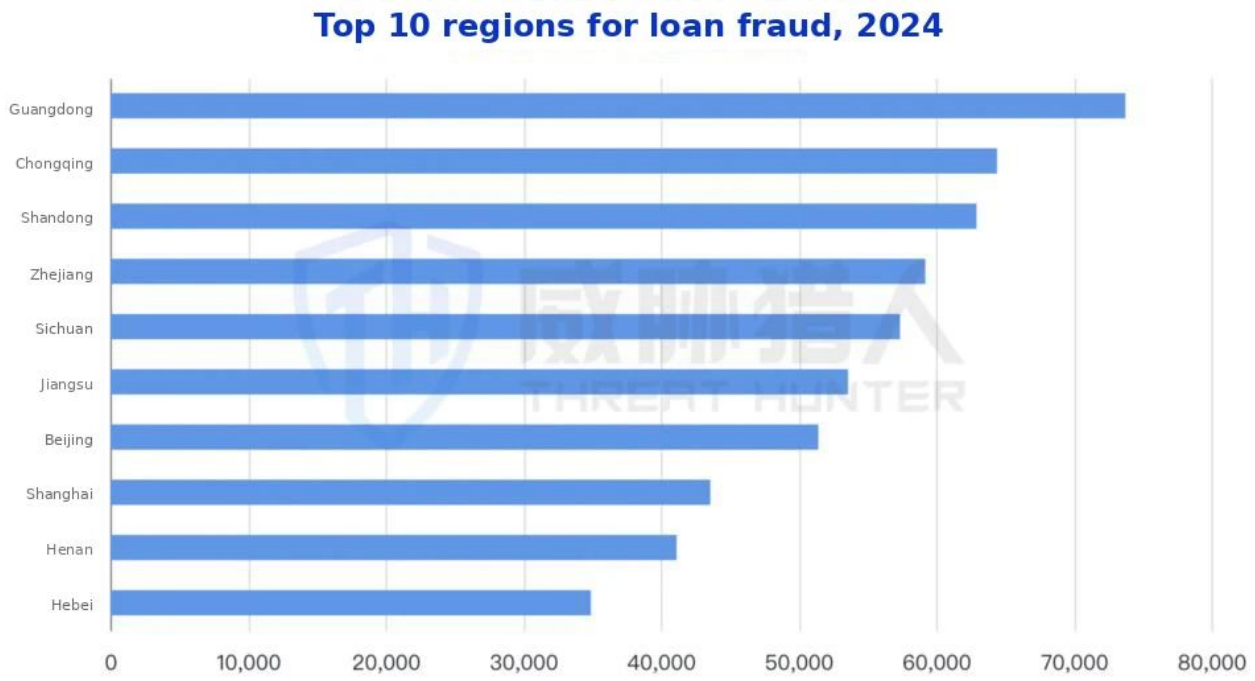


Loan fraud by product type, 2024

Source: Threat Hunter original report, page 54. Original figure with Chinese text replaced by English.

3.2.3 top 3 regional popularity of loan fraud in 2024: Guangdong, Chongqing, Shandong

From the perspective of geographical distribution, the top five regions with the hottest credit fraud areas in 2024 are: Guangdong, Chongqing, Shandong, Zhejiang, and Sichuan.



Top 10 regions for loan fraud, 2024

Source: Threat Hunter original report, page 54. Original figure with Chinese text replaced by English.

3.2.4 Professional debt: The phenomenon of “selling credit reports for money” has intensified, and threat actors are targeting high-credit and high-qualified customers.

With the continuous changes in the social and economic environment and the transformation of financial consumption culture, more and more consumers have begun to advocate "selling credit reports for money", and the popularity of "debt" continues to rise.

(1) The popularity of "debt-taking" continues to rise in 2024, and the amount of relevant intelligence in the second half of the year increased by 56% compared with the first half of the year. In 2024, Threat Hunter's capture of "debt-taking"-related attack intelligence showed an upward trend, and the popularity of "debt-taking" increased, reaching a peak in September, and the number of related intelligence in the second half of the year increased by 56% compared with the first half of the year.

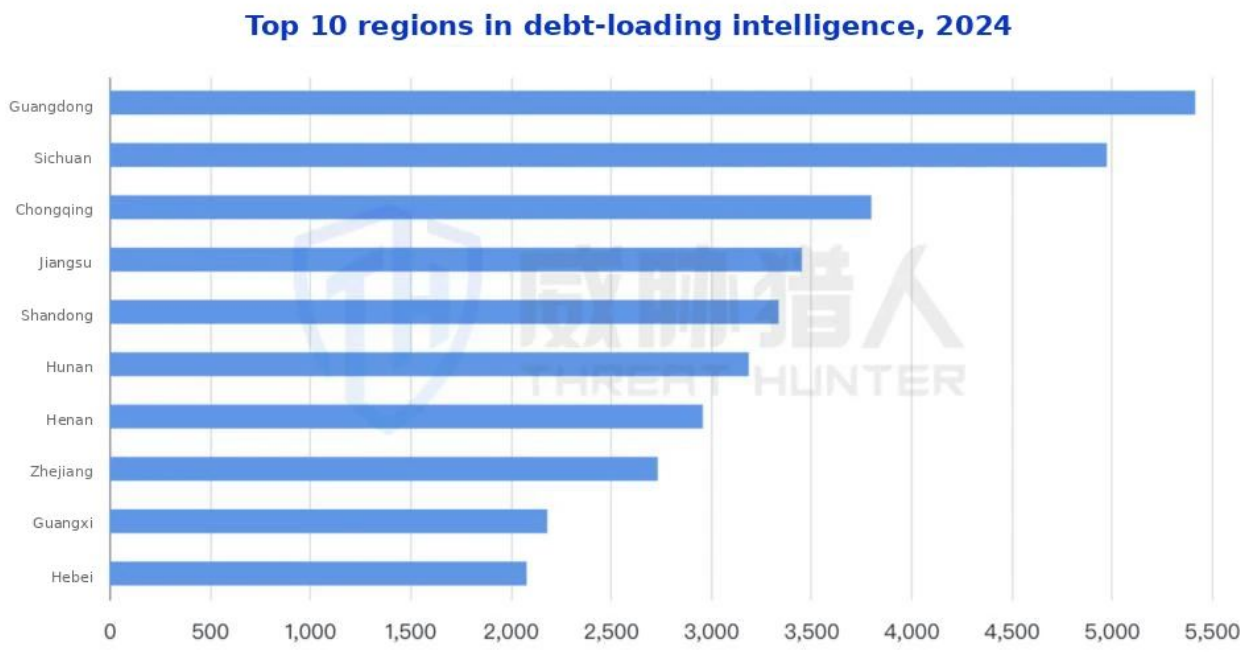


Debt-loading risk intelligence by month, 2024

Source: Threat Hunter original report, page 55. Original figure with Chinese text replaced by English.

(2) Top 3 most popular provinces for debt-incurring areas in 2024: Guangdong, Sichuan, and Chongqing. Threat Hunter intelligence data shows that in 2024, loan fraud related to "debt-incurring" will be active in the top 3 provinces (including municipalities directly under the Central Government).

They are Guangdong, Sichuan and Chongqing.

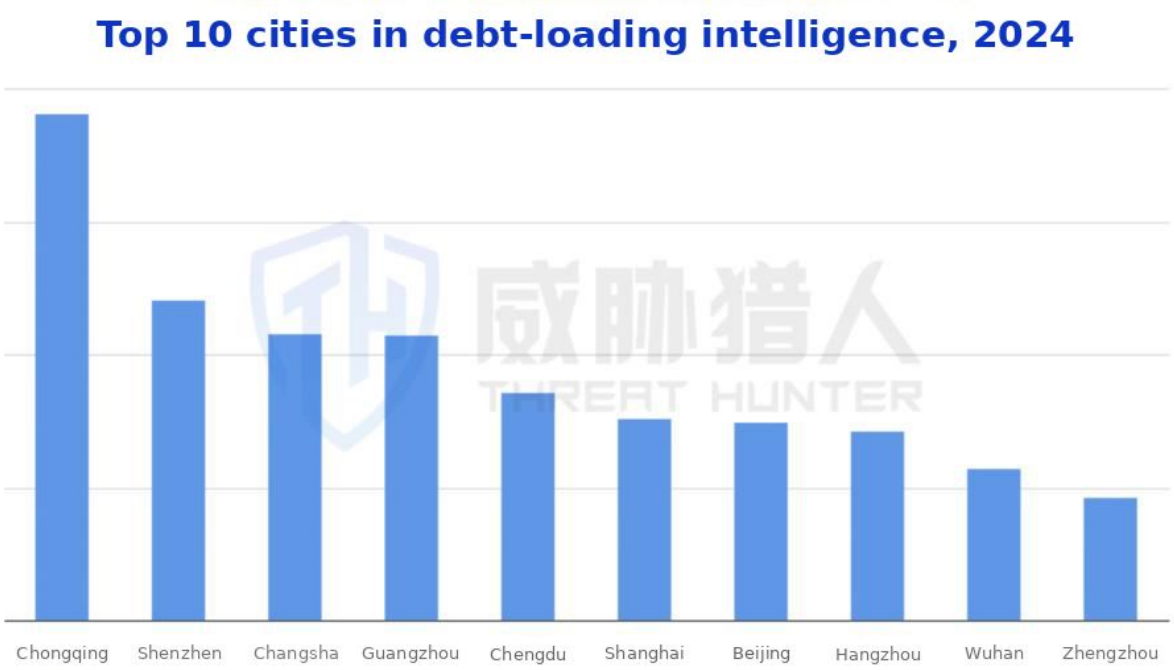


Top 10 regions in debt-loading intelligence, 2024

Source: Threat Hunter original report, page 55. Original figure with Chinese text replaced by English.

(3) Top 3 cities with the hottest debt-incurring areas in 2024: Chongqing, Shenzhen, Changsha. Threat Hunter intelligence data shows that in 2024, loan fraud related to "debt-taking" will be active in the top 3 cities (including municipalities directly under the Central Government).

They are Chongqing, Shenzhen and Changsha.



Top 10 cities in debt-loading intelligence, 2024

Source: Threat Hunter original report, page 56. Original figure with Chinese text replaced by English.

(4) threat actors are more likely to choose clients with good credit conditions, good qualifications, and good appearance. Threat Hunter research found that when threat actors choose candidates for debt, they are gradually more inclined to choose customers with good credit conditions, good qualifications, and good appearance. It is difficult for the existing anti-fraud models and scorecards of many financial institutions to identify such high-quality and high-risk customers, and the proportion of debtors who have passed automated approval is also increasing.

The selective changes in the attributes of debtors by threat actors in 2024 are mainly reflected in the following situations:

Attribute	New in 2024	Before	After
Locality	Stronger local-residence matching	Few local targets; mostly residents from anywhere in China.	Local residents (same city or province) first; residents from elsewhere second.
Age	Younger targets	Mainly middle-aged and older, 40–60.	Mainly young and middle-aged; 25–45 is most sought after.
Qualifications	Good personal qualifications	People with no assets, income or credit record; no requirements.	Clients who bring their own qualifications, ideally owning a home or car or running a business.
Appearance	Personal image matters	No requirements on looks; anyone will do.	Looks, bearing and presentation are the new standard.

How threat actors changed the debtors they target, 2024

Source: Threat Hunter original report, page 56. Table re-typeset in English from the original.

The following is some advertising information recruited by debt-ridden threat actors:

房+信。十天左右房子下来。半年出300-500。一个月左右出30+50一年出500-1000客户资质不同,出款额度也不同 年龄25-45,客户形象各方面没问题可以放宽,纯白,小白,近期不能有申请记录,半年不能有单位更新 房子下来可以配非标企业,根据客户合中介选择 ★45岁以上客户额度同比降低。房子时间20天左右★ ★跑分。案底。形象差的不要★	1.湖南籍长沙签房/信贷/企业贷:25-47岁;可只合作签房/也可房信企一条龙,房包一年月供,有返; 2.全国户籍25-46岁纯白做全国资产包,返100万起。25-55岁有房贷或信用卡的做广州信贷20-50万。 3.长沙有房,快贷10-15万/装修贷:20-30万; 4.湖南省内有执照/有流水的,可以做长沙市内商铺/别墅/房子配资融资。	一手别墅,全国,纯白、单签、双签 28-44岁、落地费!可跟单,费用全包! 四川、重庆、贵州房、信、企 年龄25-48岁、省内客户为主, 外地优质客户也可,可单签、 形象好,能说会写 会背! 三包,催单、急单不收	山东房企,山东周边户籍,返佣5-8w,信贷当月出40-60, 企业800-1000,小白,小花(查询半年不超6,总共不超10,不能有单月集中查询,负债10w以内), 年龄25-45,单身或者离异

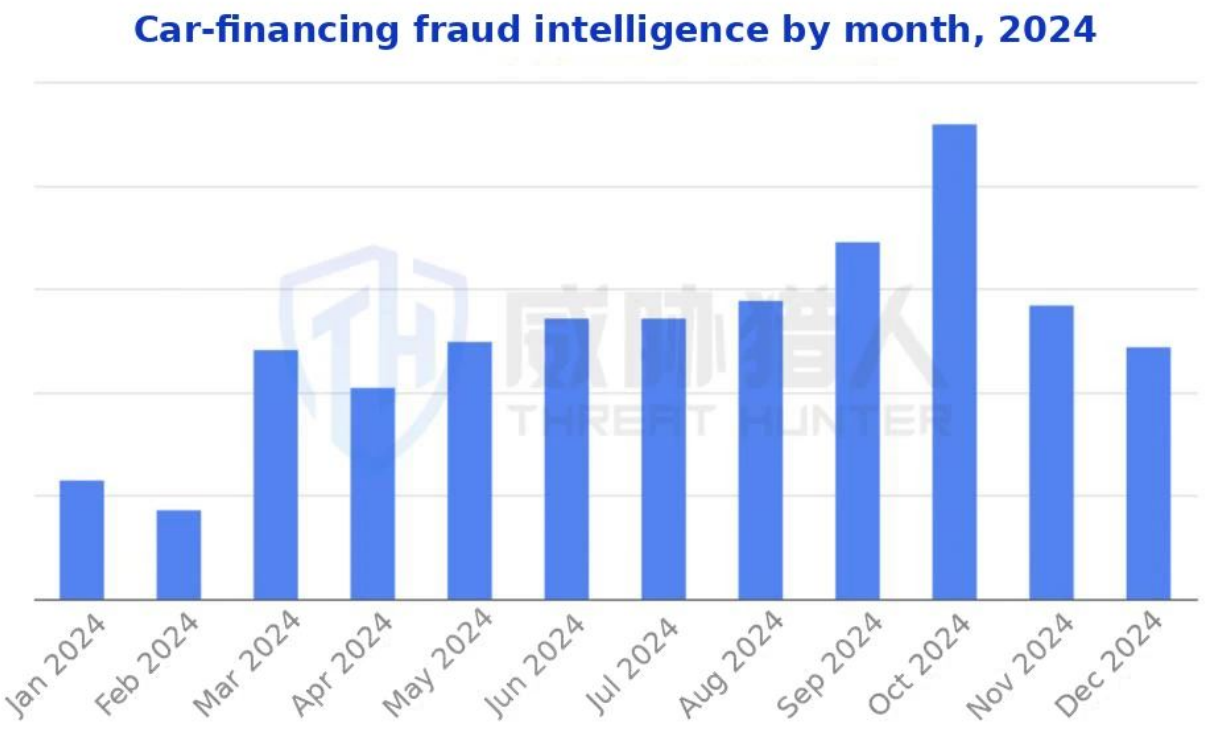
Recruitment adverts posted by debt-loading groups

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

3.2.5 Car financing fraud: The popularity of car loan fraud continues to rise, and "cash-out of car purchases" is becoming increasingly rampant

In recent years, the auto finance market has continued to expand, and auto loan fraud has become increasingly rampant. Threat Hunter's investigation found that illegal threat actors, under the banner of "financing a car," "purchasing a car with 0 down payment," and "cash out a car," recruit some people who are unable to obtain financing through normal loans but have financial needs, such as households with white credit, poor households, black households, etc., and carry out contract fraud and loan fraud by "fake car purchases, real cash out" through identity packaging.

(1) In 2024, car-financing-related attack intelligence showed an upward trend, and public opinion on car-financing risks in the second half of the year increased by 62% compared with the first half of the year.



Car-financing fraud intelligence by month, 2024

Source: Threat Hunter original report, page 57. Original figure with Chinese text replaced by English.

(2) Top 3 cities for car financing fraud intelligence in 2024: Shenzhen, Chongqing, Baoding (3) Car financing fraud techniques and manifestations Threat Hunter research found that threat actors gather some people who have no loan qualifications but have financial needs. With the organization, advance, packaging and customer cooperation of the threat actors chain, one person can apply for multiple car loans, and one car can also apply for loans from multiple financial institutions.



Top 10 cities in car-financing fraud intelligence, 2024

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

Fraud method	Form	Details
Document packaging	Identity packaging	Fake or real packaging. Fake: false employer, false social-insurance and housing-fund records, personal-tax app packaging of the job, and so on. Real: actually buying a home, really taking over a company, really paying social insurance and housing fund, or paying money into the client's salary card on a schedule as wages.
Document packaging	Income and statement packaging	Fake bank statements and income records from fake housing-fund, personal-tax, bank and payment apps.
Document packaging	Car insurance and invoice packaging	Inflate the loan with false invoices; insure an expensive car and borrow to buy it while actually buying a cheap car and cashing out.
Loan method	Several loans per person or per car	One person takes out loans on several cars, or one car is used for loans at several lenders.
Borrowing in another's name	Proxy-name and proxy purchases	Threat actors talk or trick clients into taking paid car loans, such as lending their name, fronting a purchase or "buy a car, job included" schemes.

Car-financing fraud methods

Source: Threat Hunter original report, page 58. Table re-typeset in English from the original.

For more details on car loan fraud, please see: [threat actors big data] Deconstruction of the car loan fraud industry chain

3.2.6 Non-standard loans: Material packaging loan fraud is prevalent

Threat Hunter research found that some people are unable to apply for loans normally due to problems such as incompatible qualifications and lack of conditions, and will use "fake data" such as false job information and false turnover to achieve the purpose of borrowing.

(1) The popularity of material packaging fraud will be on the rise in 2024, with the popularity in the second half of the year increasing by 148% compared with the first half of the year (2) Types and methods of material packaging fraud



Document-packaging fraud intelligence by month, 2024

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

Packaging type	Method	Where it is used
Housing-fund packaging	Fake housing-fund apps; back-paid housing-fund contributions	In consumer and salary loans, some threat actors use fake housing-fund apps to create fake fund data, or fake an employment relationship and really back-pay contributions, so that people who need money but do not qualify can obtain personal credit fraudulently. Through this packaging they help clients get several large personal loans online and offline.
Statement packaging	Paper/PDF statements; statements from copycat apps; fake statements in official bank apps	Fake statements can be used for any loan that checks personal or business income to judge repayment ability, such as mortgages, car loans and business loans. Face-to-face signing and online document top-up steps are the main targets. Threat actors supply custom fake personal and business statements so clients pass loan approval and get higher limits.

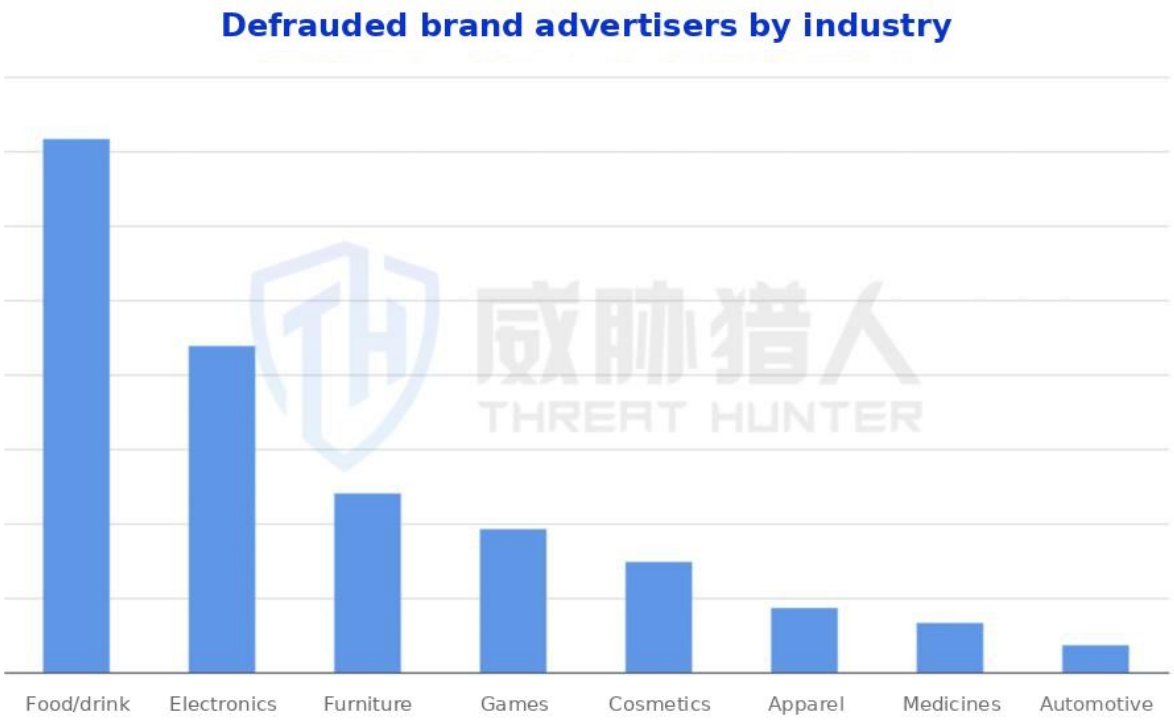
Types of document packaging in loan fraud

Source: Threat Hunter original report, page 59. Table re-typeset in English from the original.

3.3 Brand advertising fraud scenario

3.3.1 Among the brand advertisers that suffered from fraud, the food and beverage category has become the largest advertiser that suffered from advertising fraud.

Threat Hunter has captured a large amount of advertising fraud data based on advertising traffic monitoring, involving multiple industries, including food and beverages, consumer electronics, etc. The food and beverage industry is still the largest advertiser suffering from fraud.



Defrauded brand advertisers by industry

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

The ranking of advertiser brands that have suffered advertising fraud is as follows:



Advertiser brands hit by ad fraud, ranked

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

3.3.2 From the perspective of fraudulent advertising forms, the proportion of fraudulent advertising that has been played 100% reached 70.02%

Judging from the forms of fraudulent advertisements in the captured data, 15-second video advertisements are the dominant form of fraudulent advertisements, accounting for more than 99% of the total amount of captured fraudulent advertisements.

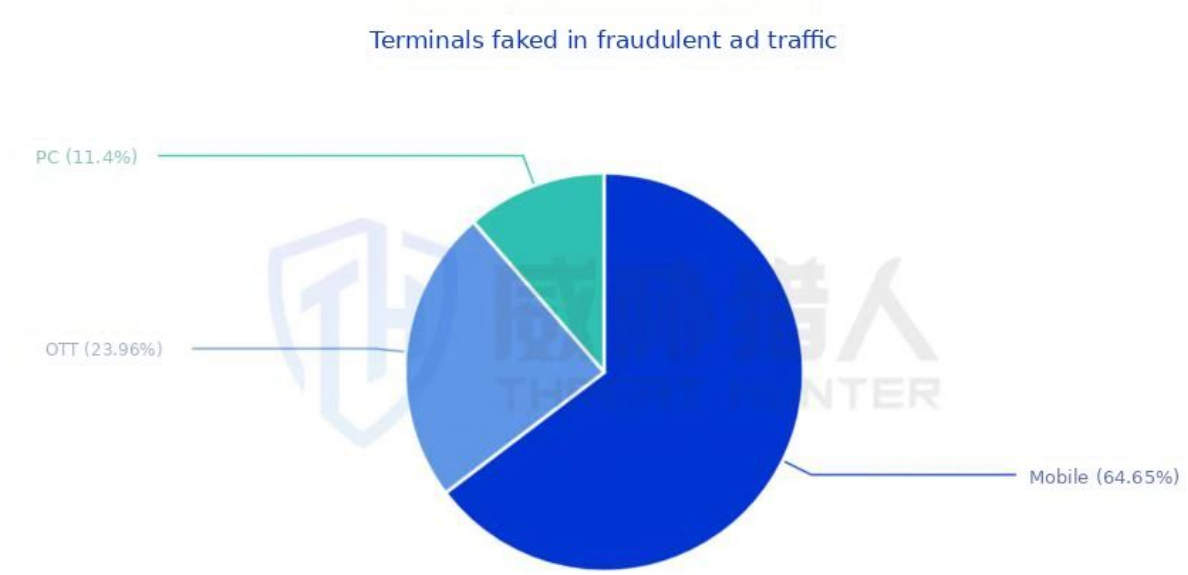
Judging from the playing situation of fraudulent advertisements, most of the advertisements that were forged and reported by devices were completely played, and the proportion of 100% played reached 70.02%. This data is obviously not in line with the behavior of normal users. In reality, not many users have the patience to finish watching the advertisements.

Video advertisements include stages such as starting to play, playing during playback, and completing playback. Ads are tracked at different stages and the traffic is reported to the ad monitoring platform. In fact, these ads are not played, but false ad playback status is faked through device swiping, and the false tracking status is reported.

3.3.3 The terminals for brand advertising counterfeiting are mainly mobile terminals

In the fraud link of advertising fraud, the reported fraudulent advertising traffic often contains dynamically changing fake device parameter information, simulating real device information and the data of displaying advertisements to deceive advertisers.

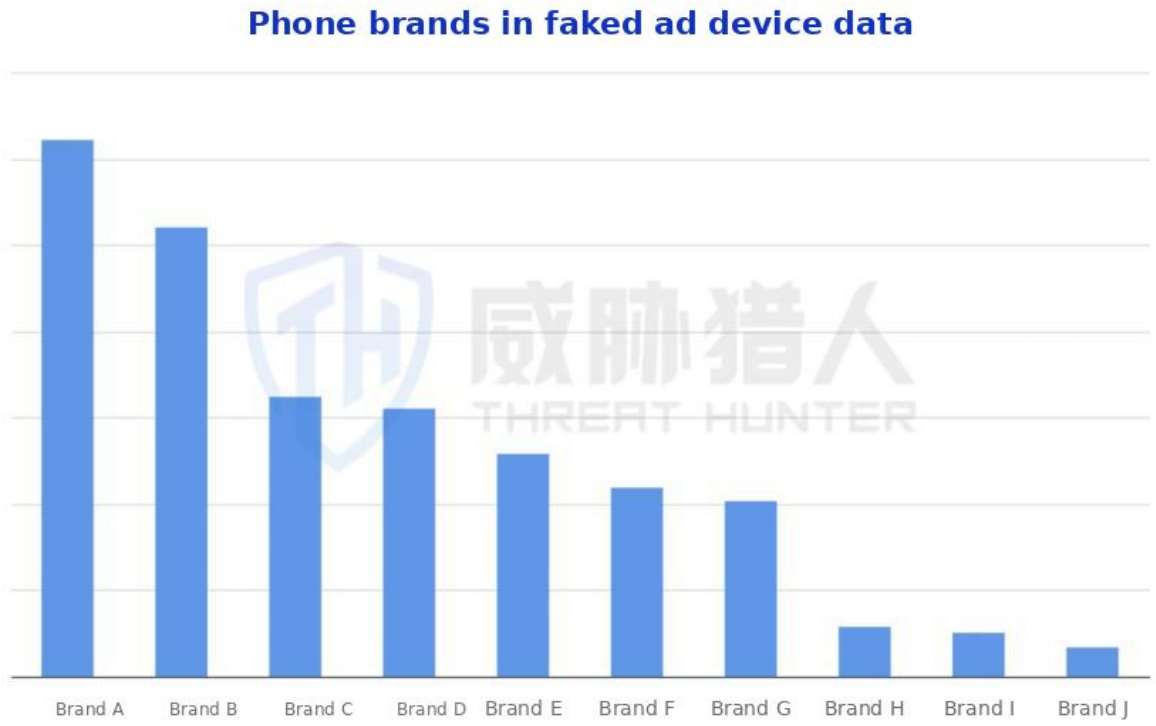
Threat Hunter analyzed the forged advertising playback data and found that the forged and reported false advertising data covered three major types of terminals: mobile terminals, OTT terminals, and PC terminals.



Terminals faked in fraudulent ad traffic

Source: Threat Hunter original report, page 62. Original figure with Chinese text replaced by English.

Further analysis found that the forged mobile terminals included mobile phones and tablets, with mobile phones being the main ones covering multiple mobile phone brands.



Phone brands in faked ad device data

Source: Threat Hunter original report, page 62. Original figure with Chinese text replaced by English.

The counterfeit OTT terminals in the advertisement include smart TVs, TV boxes, smart screens, smart speakers (with screens), singing machines, projectors, etc., covering multiple OTT terminal brands.



Smart-terminal brands in faked ad device data

Source: Threat Hunter original report, page 62. Original figure with Chinese text replaced by English.

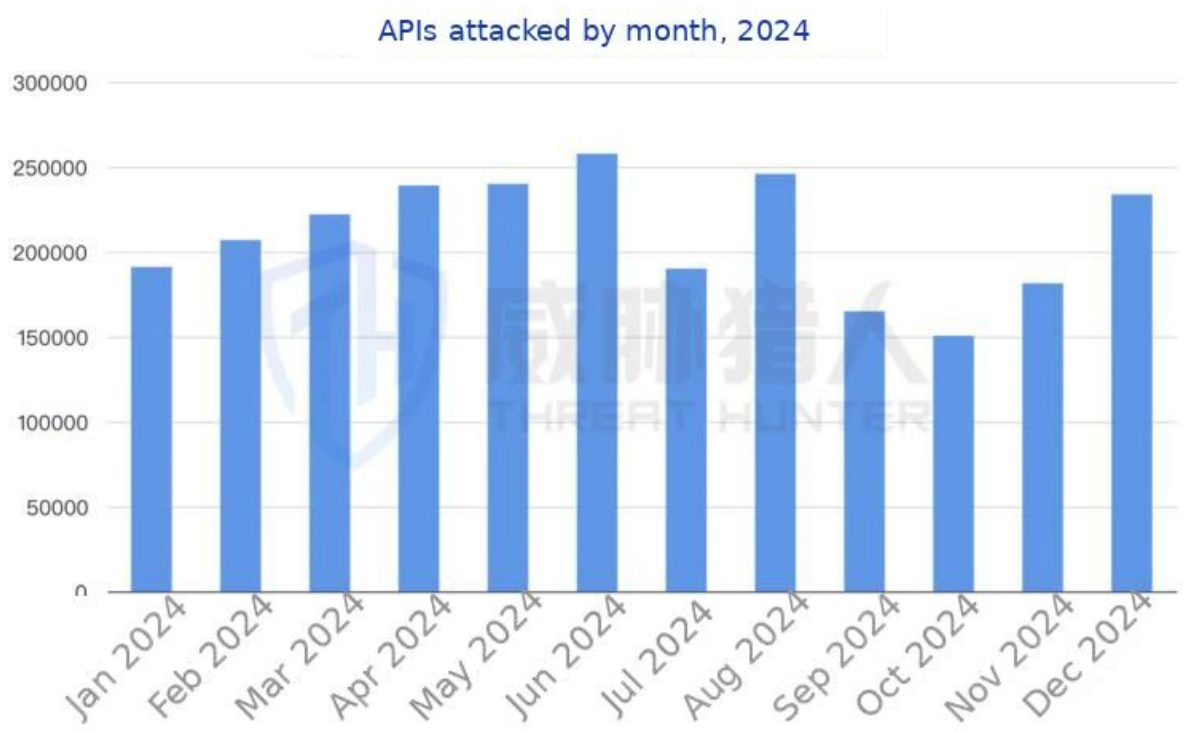
3.4 API attack scenarios

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 under attack in 2024 exceeded 2.5 million, involving audio and video, software applications, automobiles, e-commerce, government affairs and other industries.

3.4.1 The average number of APIs attacked every month in 2024 exceeded 210,000

Threat Hunter intelligence data shows that the average number of APIs attacked per month throughout 2024 exceeded 210,000.

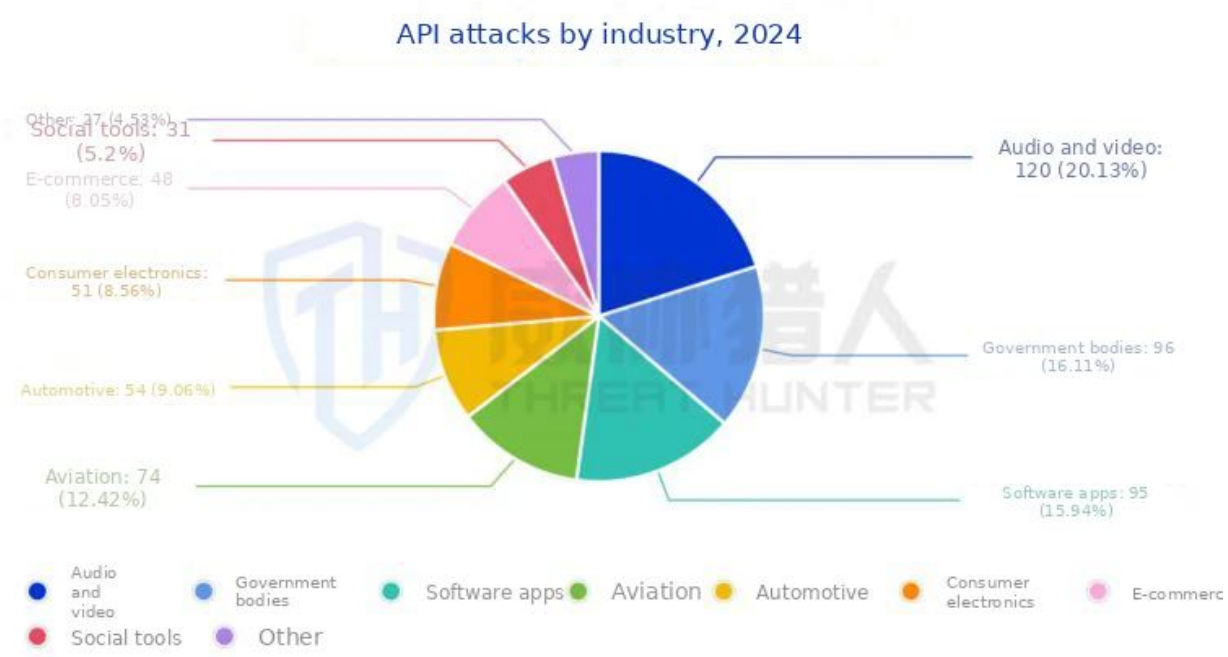


APIs attacked by month, 2024

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

3.4.2 The industry distribution of API attacks in 2024 is mainly distributed in audio and video, government agencies, and Internet software applications

Judging from the industry distribution data of API attacks in 2024, the audio and video industry is the most attacked. threat actors use APIs with security flaws on audio and video platforms to illegally crawl content, user information and other data, and obtain high profits by selling audio and video content or user information, such as illegal distribution, resale, copyright infringement, and using user information to conduct phishing attacks, fraud, etc.



API attacks by industry, 2024

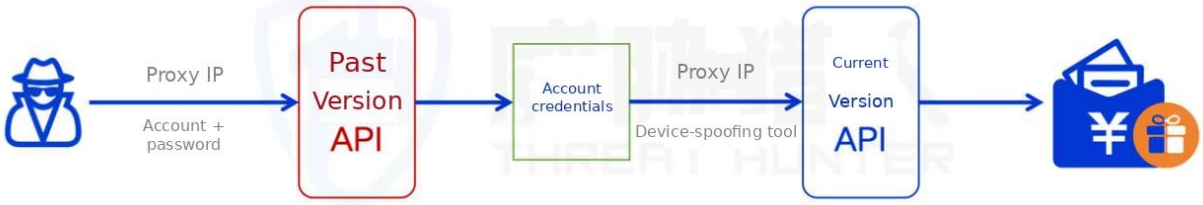
Source: Threat Hunter original report, page 63. Original figure with Chinese text replaced by English.

3.4.3 Typical API attack events worthy of attention in 2024

(1) Marketing fraud: There are security risks in the login API of an Internet platform, and corporate marketing products have been harvested. In September 2024, the Threat Hunter risk intelligence platform detected that attackers launched batch login attacks on a domestic Internet platform, using a historical version of the login API interface to obtain user credentials, and then accessing the "current version application" to use points to redeem goods for free, causing losses to the enterprise.

From the attack traffic captured by the Threat Hunter honeypot, it was found that from September to November 2024, the attacker used the proxy IP to launch more than 130,000 attacks on the historical version of the login API, and more than 100,000 accounts used points to redeem goods.

As shown in the figure below, the account and password parameters in the login API interface are not encrypted and are transmitted in clear text. The lack of simple human-machine verification methods makes it the main target of batch login attacks launched by threat actors.



Login API abuse: account and password sent unencrypted

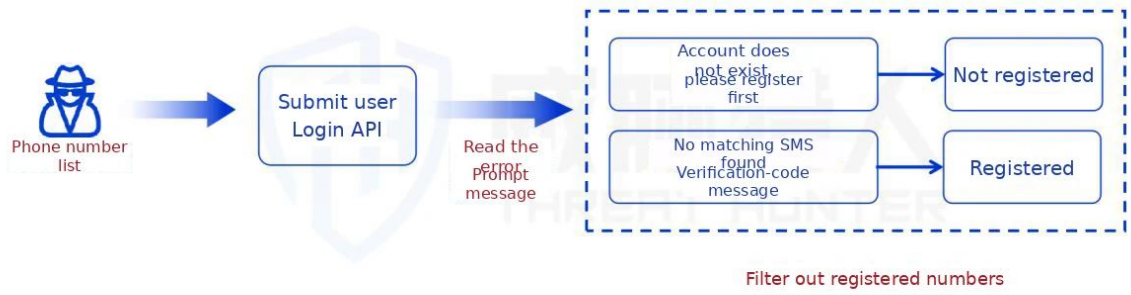
Source: Threat Hunter original report, page 64. Original figure with Chinese text replaced by English.

(2) Data crawling: A bank’s online business suffered a cybercrime ecosystem account scanning attack, and a large amount of user information was leaked

In June 2024, the Threat Hunter risk intelligence platform detected that an attacker launched an account scanning attack on a domestic bank. After traffic analysis and recurrence, it was found that the bank's asset interface had an "unreasonable error message vulnerability". threat actors could verify whether the phone number information was a registered user of the platform, resulting in the exposure of valid accounts, leakage of user privacy, and threats to system security.

Attack traffic captured from the Threat Hunter honeypot found that in June 2024, attackers launched more than 240,000 attacks on the bank's asset interface within a week, resulting in the exposure of a large number of valid accounts.

As shown in the figure below, threat actors construct the request body and use different phone numbers, while other authentication parameter information characteristics remain unchanged, such as verification code id, operation record variables, etc. If the phone number is an invalid account, the echo "The account does not exist, please register and log in". If the phone number is a valid account, the platform echoes "The corresponding SMS verification code information was not found." threat actors can use the echo to determine whether the phone number is a valid account.



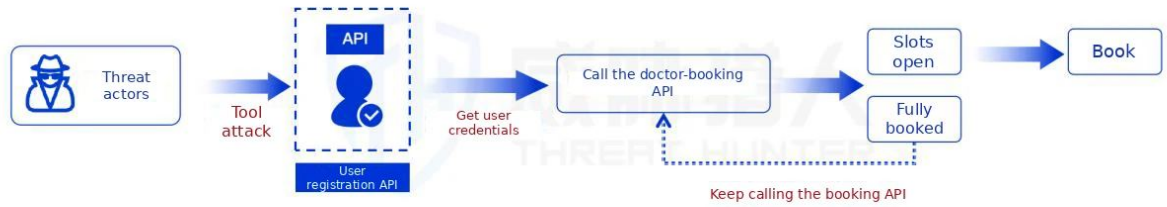
Account scanning through a bank login API

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

(3) Scalpers grab accounts: The hospital's online registration business was grabbed by scalpers, and medical resources were seized. In October 2024, the Threat Hunter risk intelligence platform detected that attackers registered in batches for a large hospital. After registration, they accessed doctor registration information and grabbed accounts, seizing medical resources.

By analyzing the traffic captured by the Threat Hunter honeypot, it was found that the attacker used a large number of illicit SIM cards to register in batches, pretended to be normal patients, and then used the registered account to log in. After logging in, he began to continuously access doctor registration information and make appointments to grab appointments.

As shown in the figure below, since the registration interface does not limit the access frequency, the attacker can continuously obtain the doctor's registration information and grab the doctor's registration immediately.



Scalpers grabbing hospital appointment slots through APIs

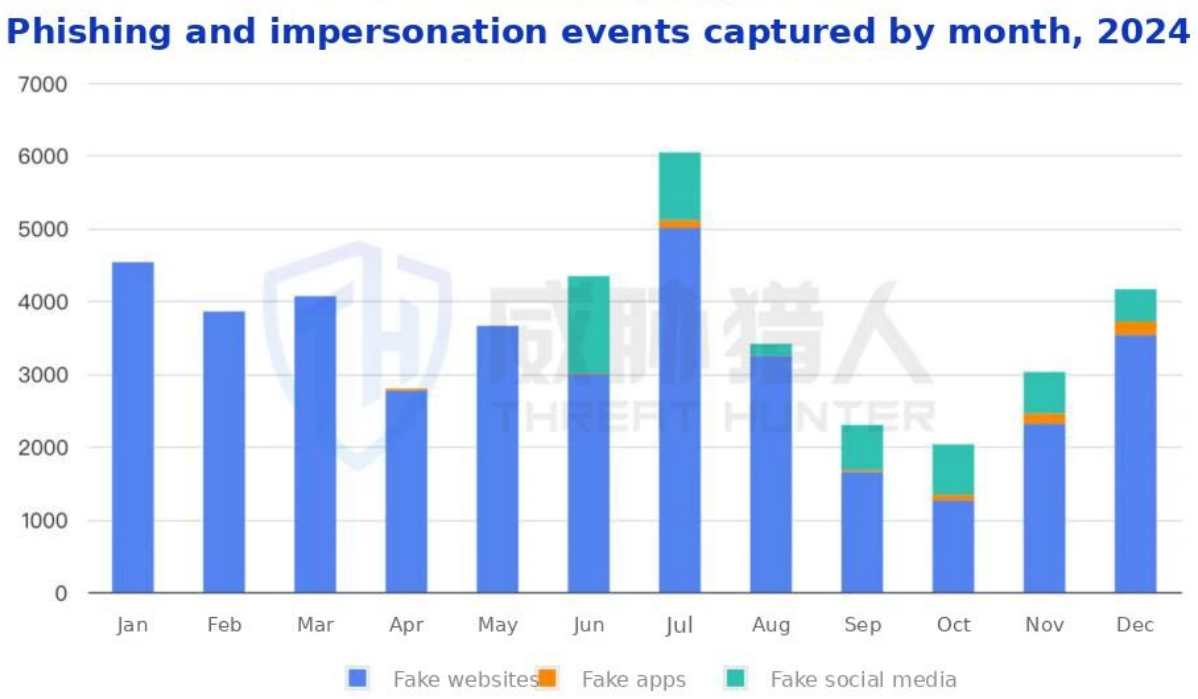
Source: Threat Hunter original report, page 66. Original figure with Chinese text replaced by English.

3.5 Phishing and Counterfeiting Scenario

3.5.1 The number of phishing and counterfeiting risk events monitored throughout 2024 exceeded 40,000, affecting hundreds of companies

In 2024, Threat Hunter monitored a total of 44,640 cases of phishing counterfeiting risk events, involving 671 companies, an increase of 150% compared with the total number of monitoring in 2023, and the overall trend of continued growth.

Compared with last year, Threat Hunter has further strengthened its monitoring of counterfeit social media this year, adding a number of new mainstream platforms to comprehensively improve its monitoring capabilities from the perspective of channel diversity, monitoring depth and coverage, and provide enterprises with broader risk protection support.

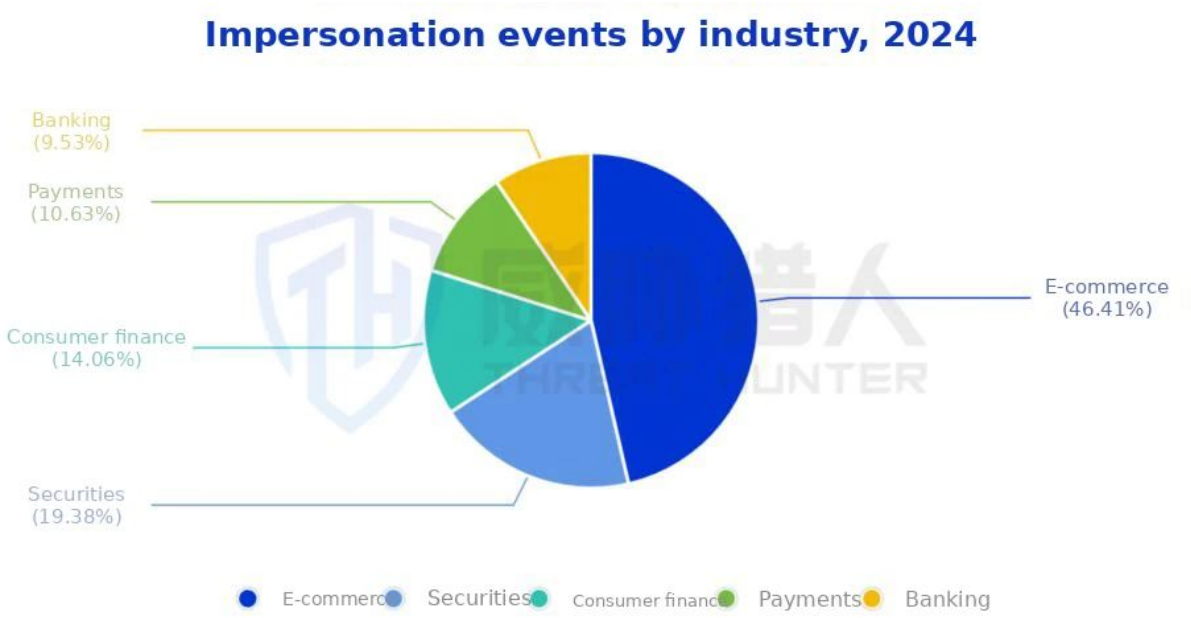


Phishing and impersonation events captured by month, 2024

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

3.5.2 E-commerce platforms have become the hardest hit area for phishing and counterfeiting, accounting for 46.41% of the incidents

Judging from the industry distribution data of phishing and counterfeiting incidents in 2024, the top three industries in which phishing and counterfeiting are accounted for are e-commerce, securities industry and consumer finance industry. Among them, the e-commerce industry has become the most serious industry for phishing and counterfeiting, with risk cases related to counterfeiting in the e-commerce industry accounting for 46.41% of the total.



Impersonation events by industry, 2024

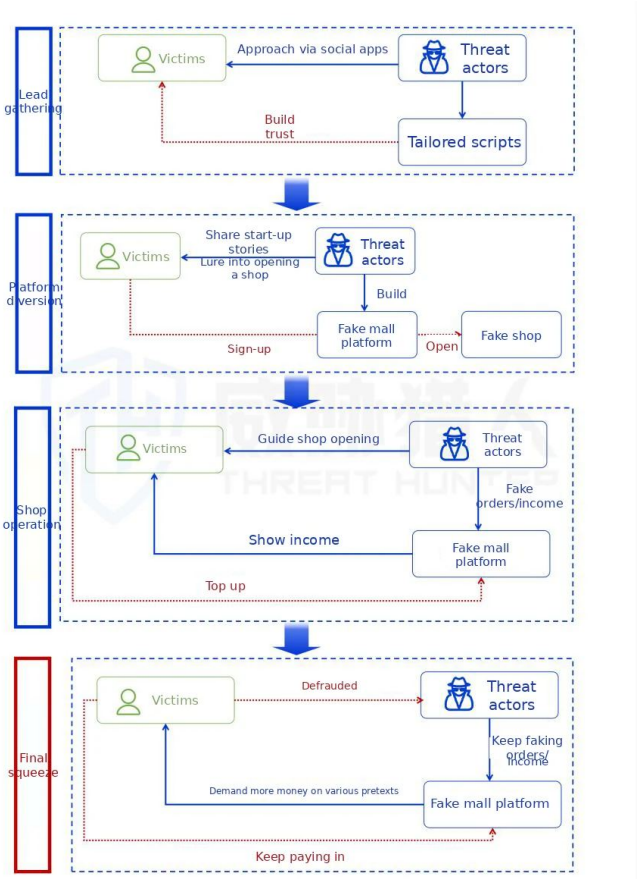
Source: Threat Hunter original report, page 67. Original figure with Chinese text replaced by English.

3.5.3 "Fake cross-border mall" fraud occurs frequently, and "counterfeit e-commerce platforms" are the main promoters

With the boom in cross-border trade, international e-commerce platforms have introduced low-threshold policies to attract novice sellers, resulting in the influx of a large number of inexperienced sellers and becoming the target of scammers.

"Fake cross-border mall listing" is one of the scams under the guise of "opening an online store to start a business". Scammers pretend to be well-known international e-commerce platforms and use "zero-cost store opening" and "high-yield distribution" to attract victims to register for counterfeit e-commerce platforms for fraud. This behavior not only brings direct economic losses to merchants, but also seriously damages the brand assets of e-commerce platforms; it destroys the platform's merchant access mechanism and affects brand credibility.

The main process and role division of "fake cross-border mall listing" are as follows:



How the fake cross-border mall scam works

Source: Threat Hunter original report, page 69. Original figure with Chinese text replaced by English.

The customer acquisition stage: Scammers contact the target group through dating software and other channels to build trust with the victims.

Counterfeit platform diversion stage: Scammers share online store entrepreneurship experience and use "zero-cost store opening" and "high-yield distribution" as bait to get victims to register for counterfeit e-commerce platforms.

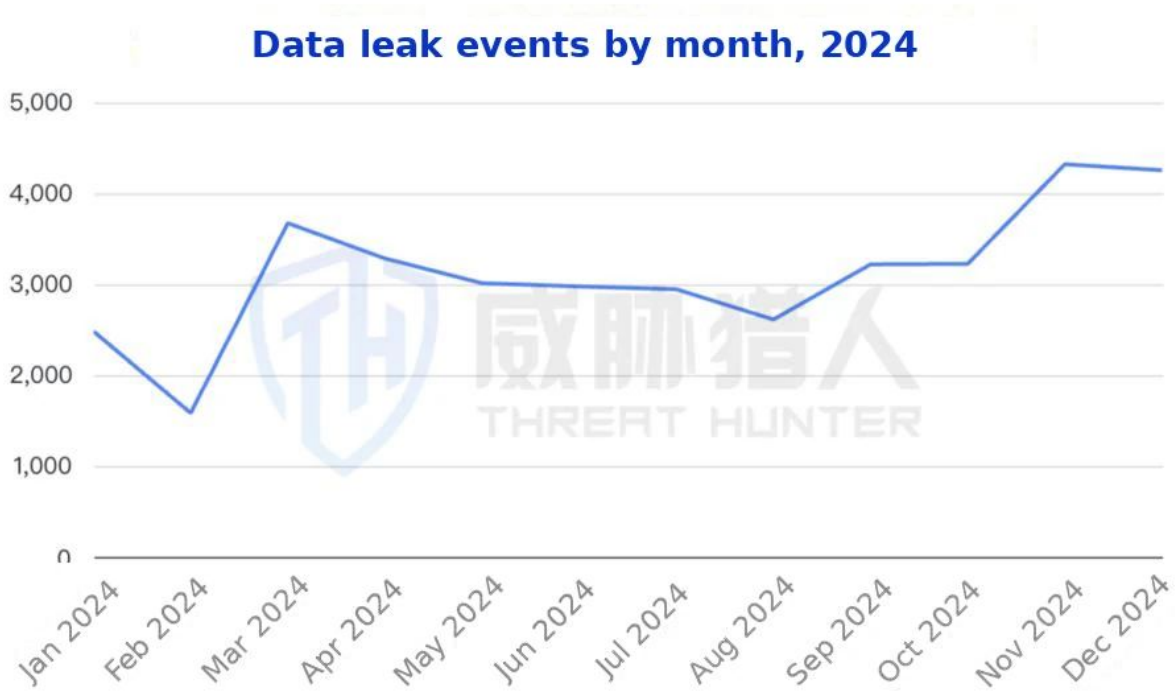
Induced store opening operation stage: After the victim registers, the scammer guides the store to open and creates the illusion of a prosperous business through virtual orders and forged profit screenshots, inducing the victim to continuously recharge and advance delivery, and gradually increase capital investment.

Fish-killing fraud stage: When the victim invests a large amount of money, the scammer uses the excuse of delaying logistics, freezing accounts, etc. to further demand payment of liquidated damages or deposits until the victim's funds are completely drained. The entire scam is disguised as a legitimate business venture, taking advantage of the victim's desire to make quick money to gradually complete the fraud loop.

3.6 Data leakage scenario

3.6.1 In 2024, 37,575 data leakage incidents were monitored, involving 2,598 companies in finance, e-commerce, express delivery and other industries.

Data from the Threat Hunter data leakage risk monitoring platform shows that from January to December 2024, the entire network monitored 303 million pieces of intelligence about data leaks. Based on the Threat Hunter authenticity verification engine and DRRC professional manual analysis, a total of 37,575 effective data leakage incidents were verified, involving 2,598 companies in finance, e-commerce, express delivery and other industries.



Data leak events by month, 2024

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

3.6.2 The risk of data leakage in the banking industry ranks first for two consecutive years, and local life enters the top ten for the first time

From the perspective of industry distribution, 88 industries were involved in data breaches from January to December 2024. The top five industries are banking, e-commerce, consumer finance, insurance and express delivery. Among them, the number of data breaches in the banking industry was as high as 6,333, making it the industry with the largest number of data breaches for two consecutive years.



Top 10 industries for data leak events, 2024

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

In addition, the industry ranking of data breach incidents in the local life industry this year has increased compared with 2023, rising from the previous Top14 to the Top10. Data shows that more than 700 data breaches were discovered in the local life industry in 2024, a sharp increase from 2023

7. 22 times.

Further analysis found that the reason for the sharp increase in local life data leakage is the new type of leakage "forced login".

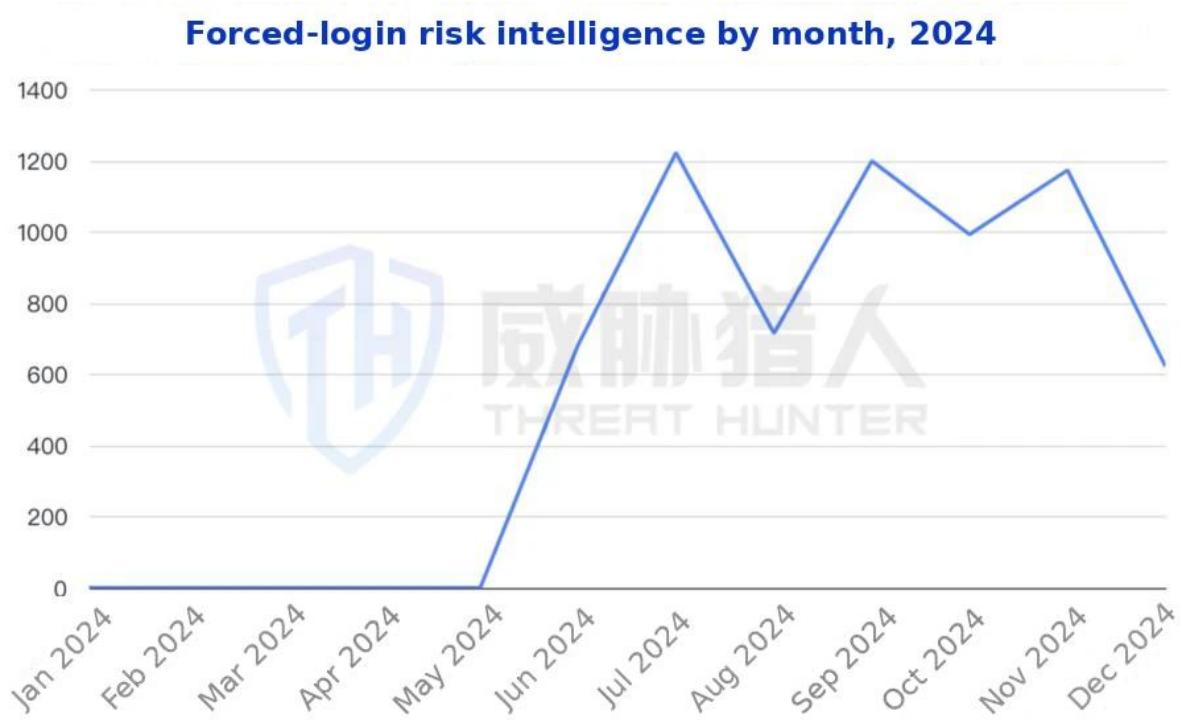
Forced login: refers to the use of technical means to force login to a user's account and obtain the private information in the user's account.

Local life: mainly refers to service platforms that provide takeout, catering, movie tickets, grocery shopping and other services closely related to life.

3.6.3 The emergence of a new type of data leakage, "Forced Login", involving leading platforms in e-commerce, takeout, express delivery and other industries

Threat Hunter discovered a new type of file check in 2024 - "forced entry". The leaked information mainly involves users' online shopping orders, takeout delivery orders, travel taxi orders, express delivery order information, etc., covering leading platforms in multiple industries such as e-commerce, express delivery, local life services (mainly the takeout industry) and travel services.

Since June 2024, methods of obtaining data through "forced login" have begun to appear, and by the end of December, there had been more than 6,600 cases. Initially, it was mainly concentrated on the leading e-commerce platform, and then gradually spread to multiple platforms such as takeout and express delivery.



Forced-login risk intelligence by month, 2024

Source: Threat Hunter original report, page 71. Original figure with Chinese text replaced by English.

Forced login: refers to the cybercrime ecosystem using a variety of complex techniques to forcefully log into the user's platform account, obtain sensitive information such as specific orders placed under the account, and then provide this information to downstream data buyers. When midstream data is sold, the sales advertisement will be marked with [forced login].

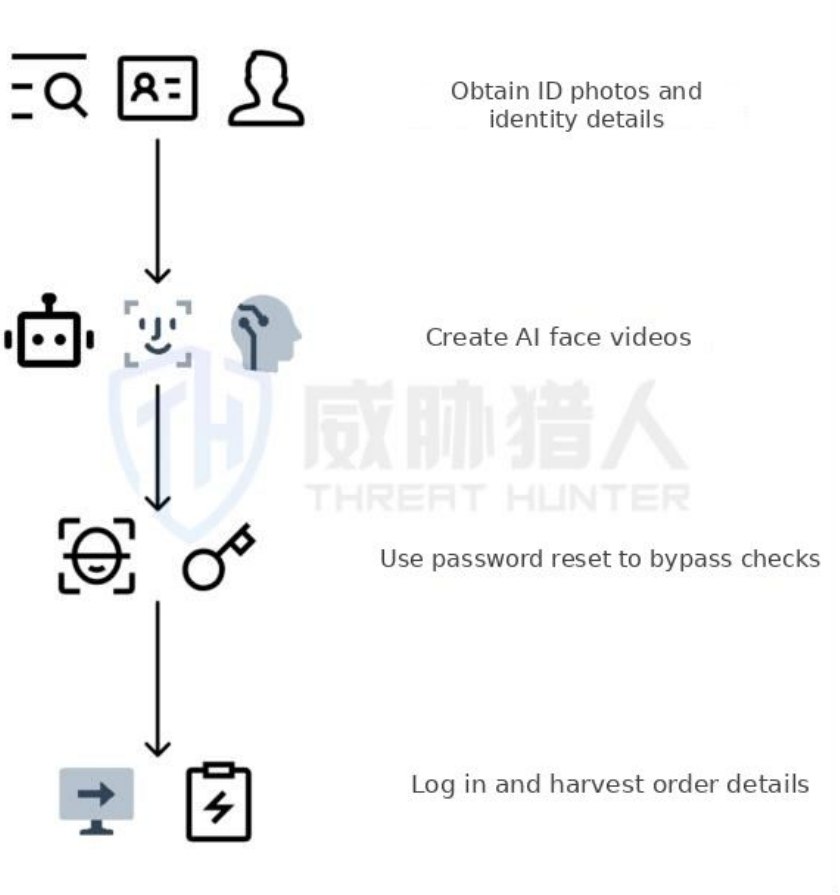
So, where did the “forced login” data come from?

Threat Hunter intelligence personnel further dug and analyzed "forced login" and found that the main modus operandi of the upstream gang against "forced login" was as follows:

Information acquisition: First, the attacker obtains the user's ID number, ID photo and other information through other channels (such as file checking or social engineering database) through the phone number.

Bypass verification: Next, use the obtained ID photo to generate an AI video or simulated face to bypass the platform's video verification link.

Forced login: Finally, through the platform's forgotten password or password retrieval interface, bypass the platform's verification mechanism, forcefully log in to the user's account, thereby obtaining sensitive information such as the order content in the account.



How "forced login" works

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

After the upstream gangs obtain order information from e-commerce, takeout, express delivery, travel services and other industries through "forced posting", the midstream gangs then publish sales advertisements in various anonymous group chats, social media, etc. to attract more downstream demand groups.



Forced-login data offered for sale

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

3.6.4 The rise of “decryption” services in the logistics industry, and related data leakage incidents have gradually increased in the past year

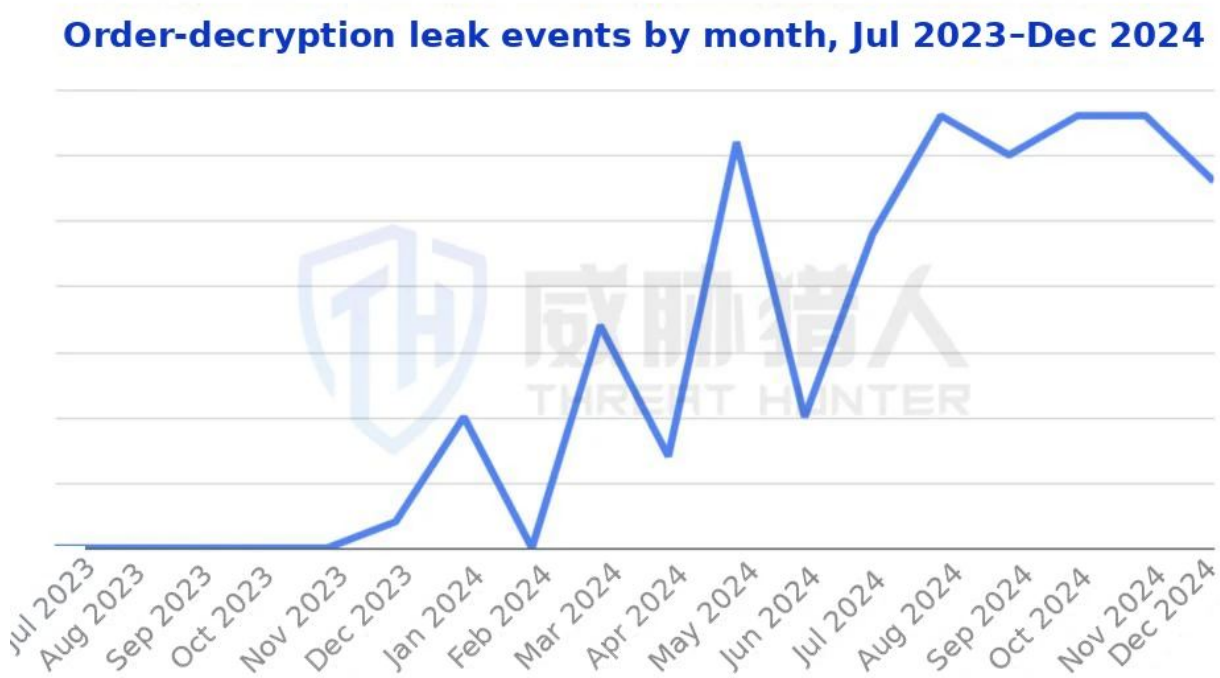
In recent years, "privacy mask" technology has been continuously developed to protect the security of personal information by hiding users' real phone numbers. In the past year, with the strengthening of supervision in the logistics industry and the joint efforts of enterprises, the promotion of privacy forms has effectively reduced the leakage of express delivery forms, and the overall governance effect has been obvious (see the figure below). But criminal tactics continue to evolve. In 2024, threat actors launched a new file checking service - "decryption" to crack the privacy form. In the past year, "decryption" related data leakage incidents have gradually increased.

Order decryption is mainly done through "express delivery number + virtual number (or phone number coded in the first three and last four)" to obtain the complete phone number.



Express waybill leak events by month, Jul 2023–Dec 2024

Source: Threat Hunter original report, page 73. Original figure with Chinese text replaced by English.



Order-decryption leak events by month, Jul 2023–Dec 2024

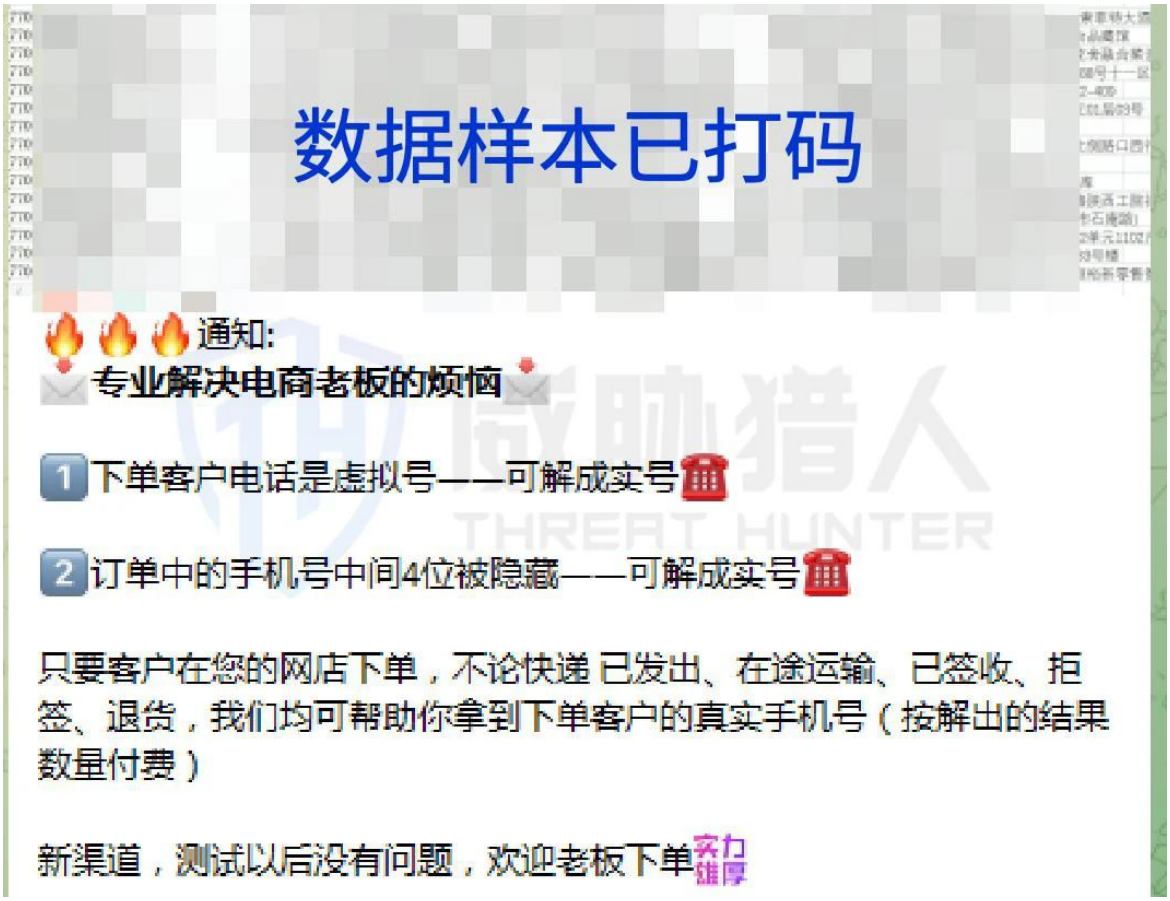
Source: Threat Hunter original report, page 74. Original figure with Chinese text replaced by English.

3.6.5 A total of 496 risk events related to the "phone platform" field were discovered in the second half of the year, a decrease from the first half of the year

Reported share: 59.90%

Threat Hunter research found that from the second half of 2023 to the first quarter of 2024, the "phone platform" field, which flags users of one major smartphone platform, appeared more often in leaked data. Judging from the chat records between the data trafficking threat actors group and downstream data buyers, the downstream data buyers' repurchase of data

The requirements repeatedly mention screening for data on users of that platform.



Leaked data requests mentioning the phone platform

Source: Threat Hunter original report, page 74. Original image retained.

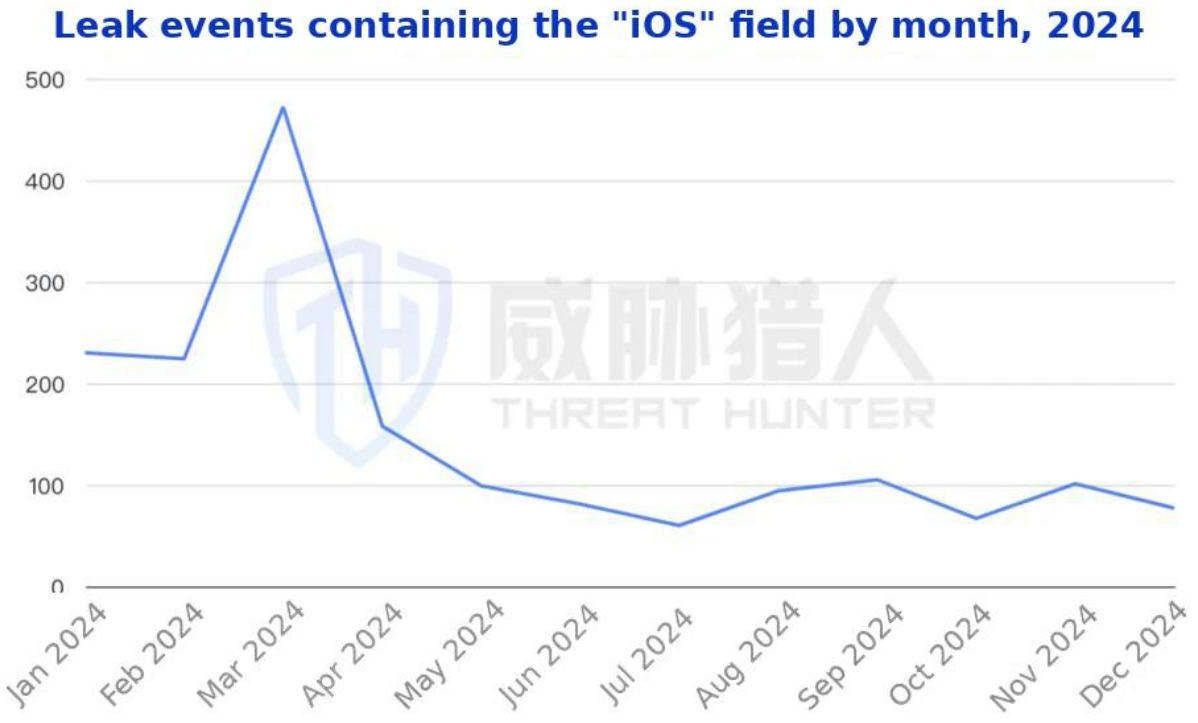


0	订单号	姓名	身份证号	手机号	出生日期	年份	性别	保障到期	投保日期	公司分部	设备信息
9	保险创建订单	34 34	石	211	195	10/27/81	1981	女	2/2/24 2	2/3/23 0	省分公司	iOS
9	保险创建订单	90 60	潘	232	360	9/25/71	1971	女	4/25/24 2	4/26/23 (	江省分公	iOS
9	保险创建订单	11 32	胡	230	458	5/3/71	1971	女	7/25/24 2	7/26/23 (	江省分公	iOS
9	保险创建订单	65 66	衣	210	097	8/20/80	1980	女	4/24/24 2	4/25/23 (	省分公司	iOS
9	保险创建订单	60 41	王	220	008	7/5/75	1975	女	10/4/24 2	10/5/23 (	省分公司	iOS
9	保险创建订单	81 14	邢	210	332	9/24/70	1970	女	4/16/24 2	4/17/2	省分公司	iOS
9	保险创建订单	25 35	朱	239	543	10/25/79	1979	女	2/21/24 2	2/22/2	江省分公	iOS
9	保险创建订单	12 05	王	230	578	10/3/67	1967	女	7/14/24 2	7/15/2	江省分公	iOS
9	保险创建订单	84 35	吕	220	707	7/26/75	1975	女	8/25/24 2	8/26/2	省分公司	iOS
9	保险创建订单	77 04	顾	210	135	2/16/73	1973	女	1/6/24 2	1/7/23	省分公司	iOS
9	保险创建订单	55 74	单	211	210	6/25/69	1969	女	7/5/24 2	7/6/23	省分公司	iOS
9	保险创建订单	31 17	杨	211	083	5/14/70	1970	女	12/11/24	12/12/	省分公司	iOS
9	保险创建订单	92 21	牛	210	235	11/14/73	1973	女	4/14/24 2	4/15/2	省分公司	iOS
9	保险创建订单	97 39	李	232	598	7/19/73	1973	女	6/12/24 2	6/13/23 (	省分公	iOS
9	保险创建订单	96 11	曲	220	511	8/16/79	1979	女	3/12/24 2	3/13/23 (	分公司	iOS
9	保险创建订单	80 28	姚	230	583	3/11/78	1978	女	7/1/24 2	7/2/23 0	省分公司	iOS
9	保险创建订单	49 84	杜	230	334	10/1/69	1969	女	12/26/24	12/27/23	省分公	iOS
9	保险创建订单	84 44	李	220	111	2/1/76	1976	女	11/4/24 2	11/5/23 (	省分公司长	iOS

Leaked data containing device information

Source: Threat Hunter original report, page 75. Original image retained.

However, starting from April, the risk events related to the "phone platform" field have shown a downward trend, and the number in the second half of 2024 decreased compared with the first half of the year.



Leak events containing the "iOS" field by month, 2024

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

Reported share: 59.90%

Threat Hunter intelligence personnel further analyzed the reasons for the decline in the second half of the year. The decline in this platform-related data in the second half of the year was mainly due to new measures the platform's maker introduced against video-call fraud.

In March 2024, the maker released a system update that lets users reject incoming video calls from unknown numbers, and in May pushed a further update that strengthened the video-call function. After testing, Threat Hunter intelligence personnel confirmed that this feature has enabled the rejection of unknown calls.

(threat actors shared the maker's official notice on rejecting video calls from unknown numbers in an anonymous group chat)



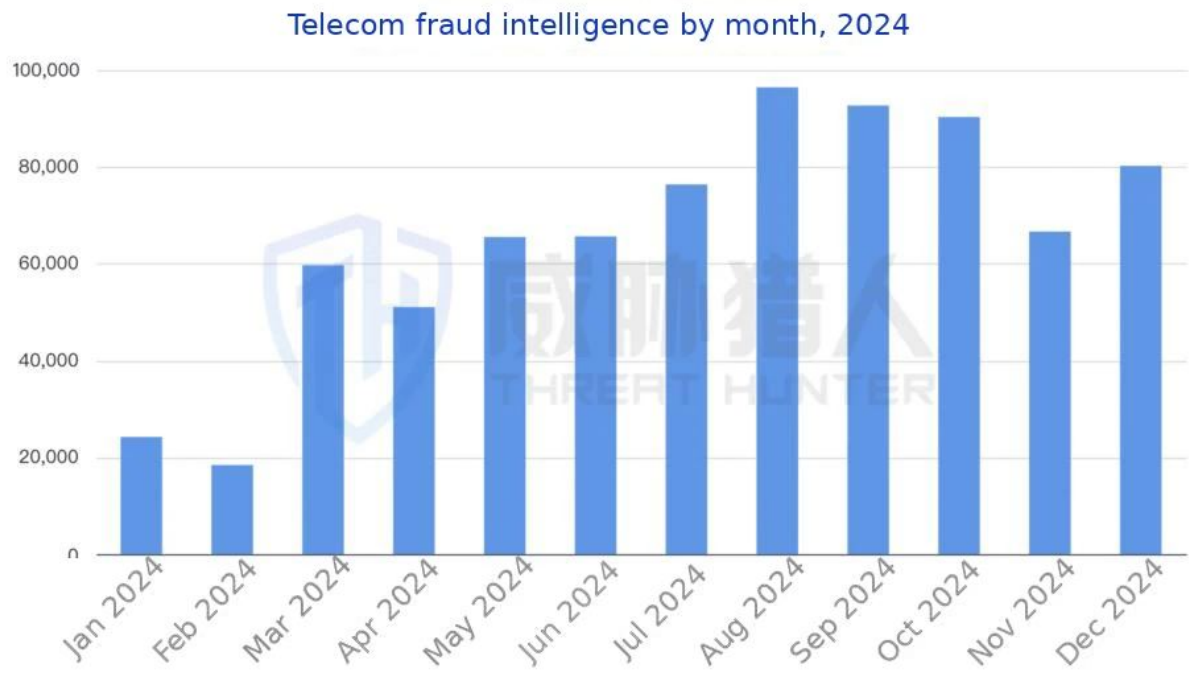
Maker notice on rejecting video calls from unknown numbers, shared by threat actors

Source: Threat Hunter original report, page 76. Original image retained.

3.7 Telecom network fraud scenario

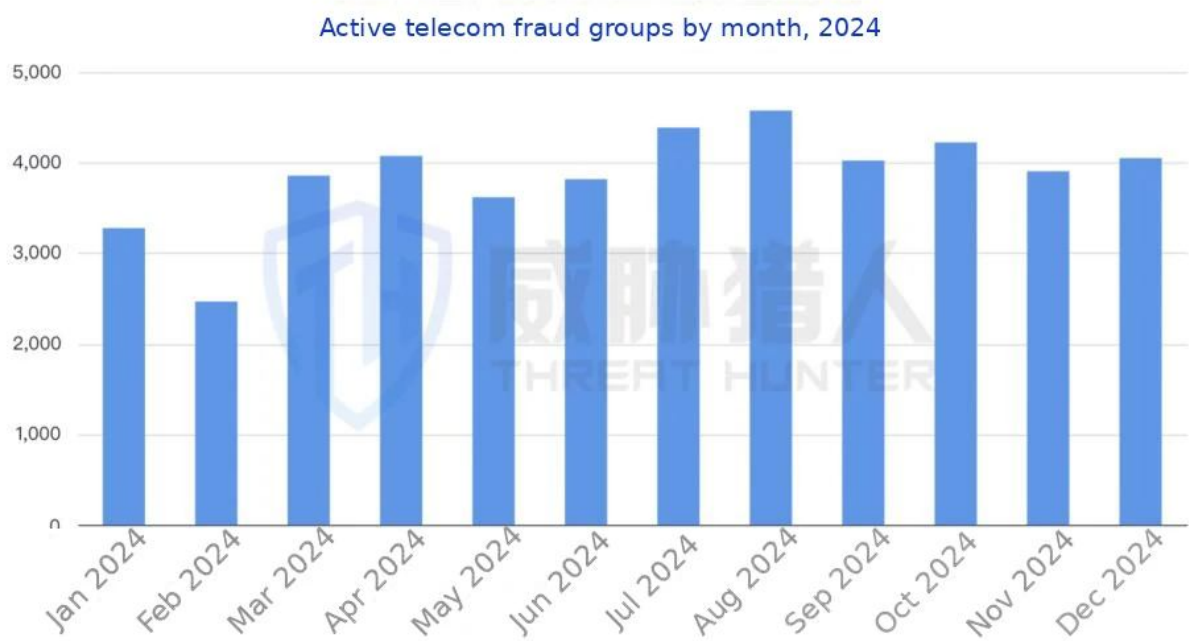
3.7.1 The fraud situation remained severe in 2024, with more than 10,000 active malicious activity groups

In 2024, the Threat Hunter risk intelligence platform monitored a total of 770,000 pieces of information related to telecom network fraud, and 10,032 active malicious activity social groups.



Telecom fraud intelligence by month, 2024

Source: Threat Hunter original report, page 76. Original figure with Chinese text replaced by English.

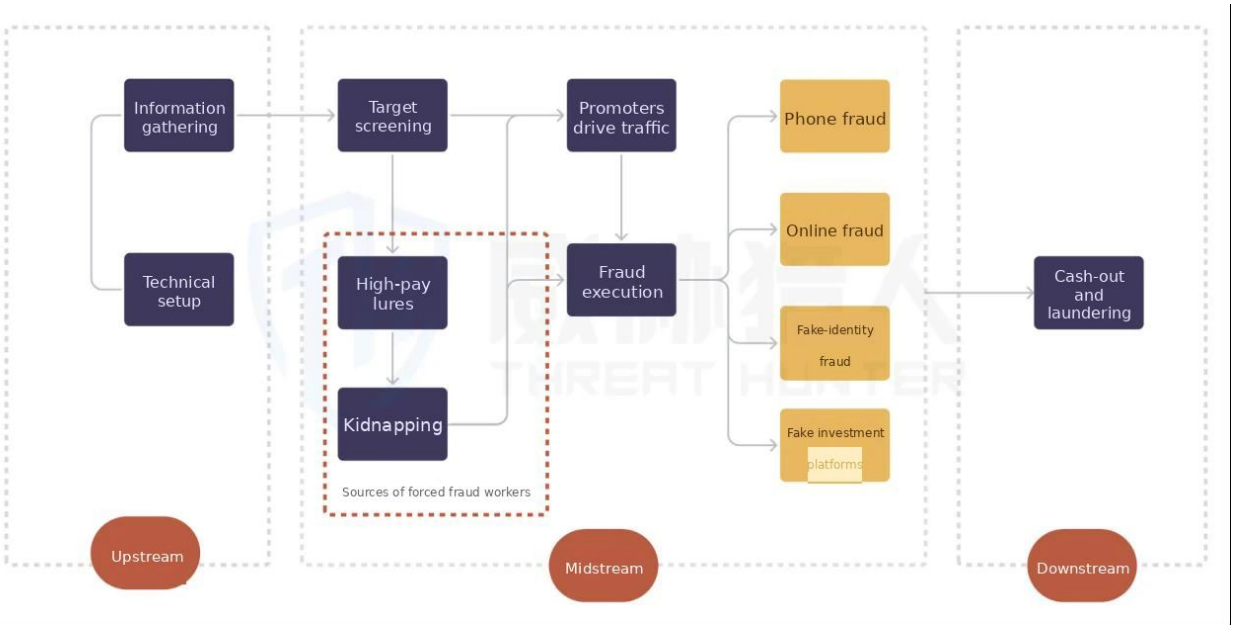


Active telecom fraud groups by month, 2024

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

3.7.2 Electronic fraud gangs work closely together and rely on sophisticated scripts to lay out various fraud traps (1) The efficient operation of electronic fraud gangs is inseparable from the close division of labor and cooperation within the gangs

Telecom network fraud has formed a mature industrial chain. There are different roles and divisions of labor within the telecom fraud gang. Members work closely together to carry out fraud activities:



Roles in the telecom fraud chain

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

Information acquisition: Fraud gangs obtain various personal information through various illegal channels. The more detailed the information, the higher the success rate of fraud.

Technical setup: The fraud team forges counterfeit websites, develops counterfeit software, and forges transaction records for subsequent fraud.

Target screening: Screen the target customer groups that are easily deceived, such as the elderly, investors, job seekers, etc., and formulate corresponding fraud strategies (scripts).

Push hands and traffic: "Push hands" refer to those people or groups that provide help or support for fraud activities. Although they do not directly participate in fraud, they contact victims and guide victims to mainstream instant-messaging apps for other fraudsters to commit fraud, that is, "push hands and traffic".

High-paying inducement: posting high-paying positions, promising generous remuneration or saying that you can earn huge amounts of money, to induce the victim to become interested in the position.

Human kidnapping: Lure the victim to the destination, tie him to an electronic fraud park, and force the victim to engage in fraud.

(2) All kinds of scams are inseparable from the underground "Scripts" designed by actors. In the early stage of the Wang Xing incident, which caused a lot of controversy recently, the fraud gang posted an audition notice from casting director Yan Shiliu in a chat group. They used the name of a famous Thai entertainment company to issue audition invitations to Wang Xing, and carefully designed a scam script that was "tailor-made" for Wang Xing (it can be seen that the fraud gang in the early stage had a very detailed grasp of Wang Xing's information, especially his career and work experience), and used Thai filming job opportunities as bait to lure Wang Xing to Thailand.

In addition to the Wang Xing incident, Threat Hunter also monitored various types of scripts, which used the specific psychological activities of different groups of people to carefully create fraud scripts that matched the characteristics and psychology of the characters. The specific cases are as follows:

Case	Target profile	Script	Fraud method	Psychology exploited	Sample lines
Case 1	Older people aged 45–65	Complete tasks to receive a large poverty-relief payment	Lure victims into installing a fake poverty-relief fund app, collect their bank card and ID details through "registration", then push them to top up in the app or help launder money under the pretext of "building transaction records".	Unfamiliarity with welfare and poverty-relief policies; weak fraud awareness	"Hello, I am calling from a poverty-relief fund. You have a relief quota and can claim your payment. Claiming is completely free and places are limited, so please add us soon. This is a government subsidy; if you do not claim it, we will assume you do not need it and you will not be on future lists. The scheme is state-funded and run from Beijing, and claiming costs nothing."
Case 2	People who want concert tickets	Insider premium tickets from a ticketing platform	Lure victims into ordering through a fake "internal link" built by the fraud gang, then take the money.	Fans' urgent need for tickets and trust in official or insider channels	"Want concert tickets? Can you accept a premium? Order directly on the ticketing platform through my internal link. These are the platform's internal premium tickets; your details are entered as usual and the premium is included, just like buying there yourself."
Case 3	Men aged 24–30 looking for thrills	Persona: married young woman who likes adult products and invites the target to a hotel	Lure the victim into booking a room and buying adult products in a fake mall built by the gang, then take the money.	Eagerness for a date or a thrill; lures such as "free local dates"	"I'm just looking for some fun. I have a family, so we keep out of each other's lives. Book a room and send me the room number and location, and I'll come over. For our safety, buy a test kit first. I can't pay for it because my husband checks my spending; otherwise I would have paid already."

Fraud scripts tailored to different groups

Source: Threat Hunter original report, page 79. Table re-typeset in English from the original.

Written at the end In recent years, the Internet cybercriminal groups have ensured the success rate of attacks by continuously improving attack technology and mining more concealed attack resources. This has caused enterprises to face greater pressure and lag in perception and defense.

For enterprises, they should realize that the confrontation with external threat actors is dynamic and continuous. They should rely on cybercrime ecosystem intelligence data based on multi-channel monitoring of the entire network in a timely manner to start tracing the source from the preparation stage of threat actors' attacks. They should know what resources or tools the attacker is preparing to use, what characteristics these resources or tools have, and what methods the attacker will use to attack the enterprise...reach the defense frontier of the attacked party before the attacker, so that the offensive and defensive confrontation can reach a situation where "the enemy has not attacked but I control it first". This is the value of intelligence, and this is the value of Threat Hunter.

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