THREAT HUNTER RESEARCH

H1 2024 Cybercrime Ecosystem Research Report

A half-year assessment of criminal-resource supply, end-to-end automation and six recurring business-attack scenarios.

Original publication: 2024-07-17
Research team: Threat Hunter Research Team
Source report: 68 pages

Original report text

This text version is reconstructed based on the 68-page original PDF, retaining the report narrative, chapters and research scope; the cover, duplicate table of contents and purely decorative pages are not repeated. Localized figures are placed in context throughout this web edition, with the original PDF retained for reference.

Preface

In the first half of 2024, the number of cybercrime operators exceeded 4.27 million. Threat Hunter monitored the number of domestic malicious phone numbers as high as 3.23 million, the number of daily active risk IPs was 11.36 million, and the number of bank cards involved in money laundering was 195,000.

In recent years, the integration of digitalization and the real economy has become increasingly in-depth. In large-scale business online scenarios, cybercriminal groups have more prominently disrupted enterprise business security. Incidents of threat actors such as malicious traffic manipulation, fraud, and financial fraud have emerged in an endless stream. The operation of threat actors in the network has gradually become more intelligent and chain-oriented, bringing real economic losses to enterprises and affecting their normal operations and long-term development. Combating cybercrime ecosystem and strengthening effective defense have become the goals and consensus of enterprises in various industries.

Threat Hunter released the "Internet cybercrime ecosystem research report for the first half of 2024", which comprehensively analyzes and analyzes the development status of the Internet cybercrime ecosystem in the first half of 2024, attack resources used by cybercriminal groups, cybercriminal groups attack technologies and scenarios, and strives to objectively present cybercrime ecosystem intelligence data to help more companies deeply and intuitively understand the cybercrime ecosystem and effectively prevent and control various attack risks.

Related noun definitions:

1. Risk IP: Also known as black IP in the industry, it refers to IP with attack risks (including malicious behaviors such as proxy and second dial);

2. Risk phone numbers: Mobile phone numbers that are at risk of being abused or stolen, such as being used by threat actors to receive text messages and carry out batch malicious attacks.

The phone number of the attack is usually captured from the SMS verification-code receiving service or card issuing platform;

3. Risk mailbox: refers to the temporary mailbox generated by threat actors for malicious registration to defraud users of important information and spread malicious messages.

Programs, etc.;

4. illicit SIM cards: refers to those who fail to register their real names or register with a false identity, and are used by criminals to commit illegal acts.

Calling cards for criminal activity;

5. SIM pool cards: refers to the network communication hardware "SIM pool" that supports simultaneous calls to multiple numbers, group text messages, etc.

Functional black phone card;

6. Interceptor card: refers to a mobile phone card that controls the sending and receiving permissions of real users' mobile phone text messages/verification codes through virus Trojans, usually capturing their own

Interception card platform;

7. Money laundering bank cards: refers to bank cards used by threat actors to launder illegal funds (legalize illegal income), such as gambling

Boji fraud gangs transfer money laundering funds through bank card consumption, transfers, etc.;

8. Gambling-related cards: refers to bank cards that are often used for recharging and collecting payments on gambling platforms, and the associated assets involve gambling money laundering.

Threat Hunter uses a combination of manual and automated methods to monitor bank card account information used for payment collection behavior from various gambling platforms;

9. Benchmark card: refers to a bank card that is active on the benchmark platform and is often used for circulation transactions of funds from various illegal sources. Threat hunting

People obtain the bank card account information in the benchmark order from the benchmark platform app through automated means;

10. Fraud-related cards: refers to bank cards that are often used in group chats of social threat actors to transfer fraudulent funds. The associated assets involve fraud.

Money laundering fraud. 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;

11. Money laundering corporate accounts: refers to bank corporate accounts used by threat actors to launder illegal funds, because corporate accounts have a collection amount

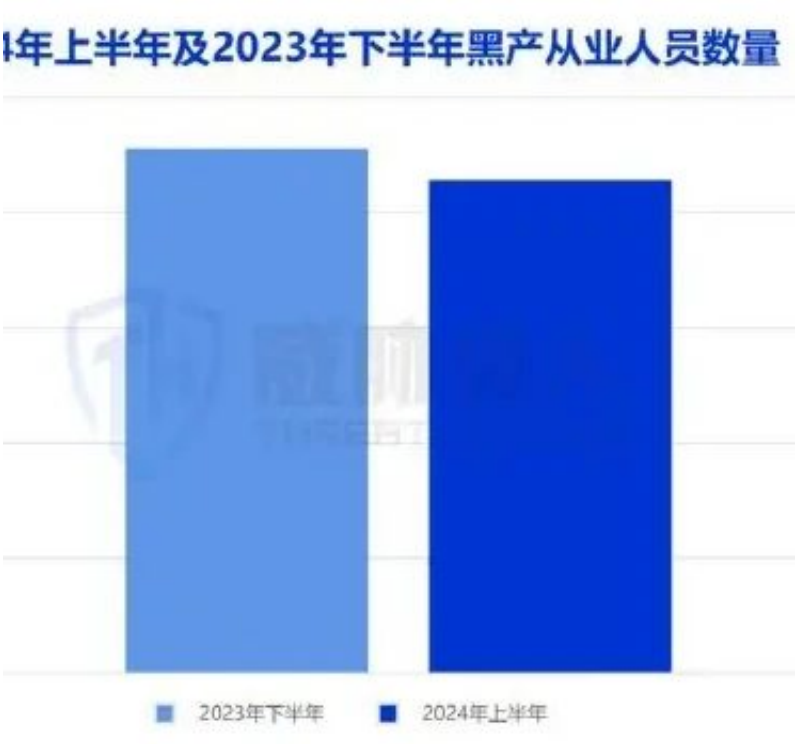
Characteristics such as large transaction volume and high number of transfers make "public accounts" often serve as concentration and divergence points for black money transfers;

12. Data leakage incidents: Threat Hunter security research experts analyze and verify samples of data leakage intelligence, etc.

Data leakage incidents confirmed to be real and valid;

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

software, configuration or authorization to log in;



2024 The number of Internet cybercrime ecosystem workers in the first half of the year was 4.27 million, compared to 2023.

Source: Threat Hunter original report, page 7

The development status of the Internet cybercrime ecosystem in the first half of 2024 The development status of the Internet cybercrime ecosystem in the first half of 2024

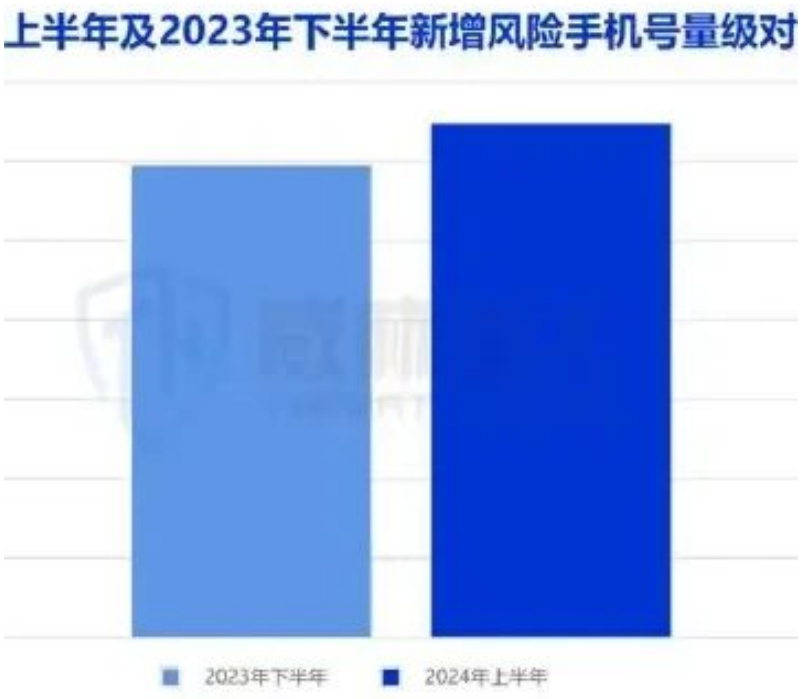
1. Development status of the Internet cybercriminal industry in the first half of 2024

1.1 In the first half of 2024, the number of Internet cybercrime operators reached 4.27 million, which is higher than that in the second half of 2023.

A half-year decrease of 6.03% Threat Hunter survey statistics found that the number of Internet cybercrime operators reached 4.27 million in the first half of 2024, a slight decrease of 6.03% from the second half of 2023.

1.2 Overview of the cybercrime ecosystem resources in the first half of 2024

1.2.1 The total number of new domestic risk phone numbers in the first half of 2024 increased by 8.8% compared with the second half of 2023



2024 Risks in the first half of the year Total IP increased by 44.8% over the second half of 2023

Source: Threat Hunter original report, page 8

According to data from the Threat Hunter risk intelligence platform, the number of domestic risky phone numbers reached 3.23 million in the first half of 2024, an increase of 8.8% compared with 2022.

1.2.2 The total amount of risk IP in the first half of 2024 increased by 44.8% compared with the second half of 2023

In the first half of 2024, Threat Hunter monitoring found that the number of daily active risk IPs continued to rise, with the number of risk IPs reaching 11.36 million, an increase of 44.8% from the second half of 2023.

1.2.3 The number of bank cards involved in money laundering in the first half of 2024 dropped by 28% compared with the second half of 2023, mainly due to the significant decrease in benchmark cards

In the first half of 2024, the number of bank cards involved in money laundering was 195,000, a decrease of 28% from the second half of 2023. Bank cards involved in money laundering mainly include benchmarking cards, gambling-related cards, and fraud-related cards. Among them, the number of new benchmarking cards has dropped the most, down 50.3% from the second half of 2023. Threat Hunter conducted in-depth research on the scoring methods of threat-actor groups and found that in the first half of 2024, the scoring groups gradually shifted from benchmarking platforms to running scores through Telegram, making monitoring significantly more difficult.

Gambling-related cards: refers to bank cards that are often used for recharging and collecting payments on gambling platforms, and the associated assets are involved in 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: refers to a bank card that is active on the benchmark platform and 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.

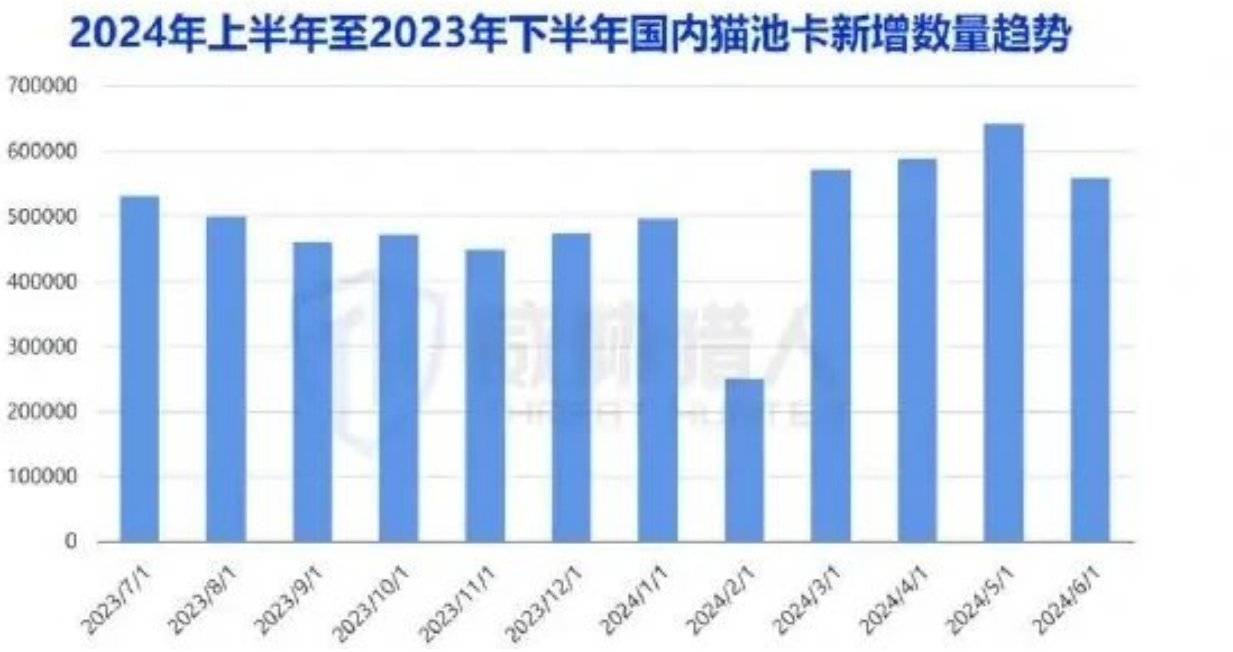
Fraud-related cards: refer to bank cards that are often used in group chats of social threat actors to transfer fraudulent funds, and the associated assets involve fraud and money laundering. Threat Hunter uses automated methods to extract bank card account information used by fraud gangs from records sent in group chats of anonymous social threat actors.

Analysis of attack resources used by threat actors in the first half of 2024

2. Analysis of attack resources used by threat actors in the first half of 2024

2.1 Analysis of risky mobile phone card resources in the first half of 2024

2.1.1 Change trend of SIM pool cards resources in the first half of 2024



2024 Trends in SIM pool card resources in the first half of the year

Source: Threat Hunter original report, page 11

(1) Domestic SIM pool cards in the first half of 2024 increased by 7.71% compared with the second half of 2023. According to data from the Threat Hunter intelligence platform, 3.09 million new SIM pool cards were captured in the first half of 2024, an increase of 7.71% from the second half of 2023.

SIM pool cards: refers to a illicit SIM cards that supports functions such as calls to multiple numbers and group text messages at the same time through "SIM pool", a network communication hardware.

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

1. In February, due to the slowdown of transactions by threat actors during the Spring Festival, the activity of downstream perpetrators decreased, resulting in a significant decline in supply, which recovered after the holiday.

Steady upward trend;

2. The decline in the number of SIM pool cards in June was mainly affected by the strengthening of fraud controls during the college entrance examination. During the college entrance examination, accounts on major platforms registered in batches.

册、恶意引流等监测力度大大加强（如不可修改账号名称、头像、介绍等），多个渠道卡商

主动反馈受该原因干扰，黑卡供给存在问题。

A source-channel notice records disruption to illicit SIM-card supply.
Source: Threat Hunter original report, page 12

2024 Trends in SIM pool card resources in the first half of the year (Chart 2)
Source: Threat Hunter original report, page 12

Monitoring efforts such as registration and malicious traffic diversion have been greatly strengthened (for example, account names, avatars, introductions, etc. cannot be modified). Many

channel card dealers have actively reported that they are affected by this reason and there are problems with the supply of black cards.

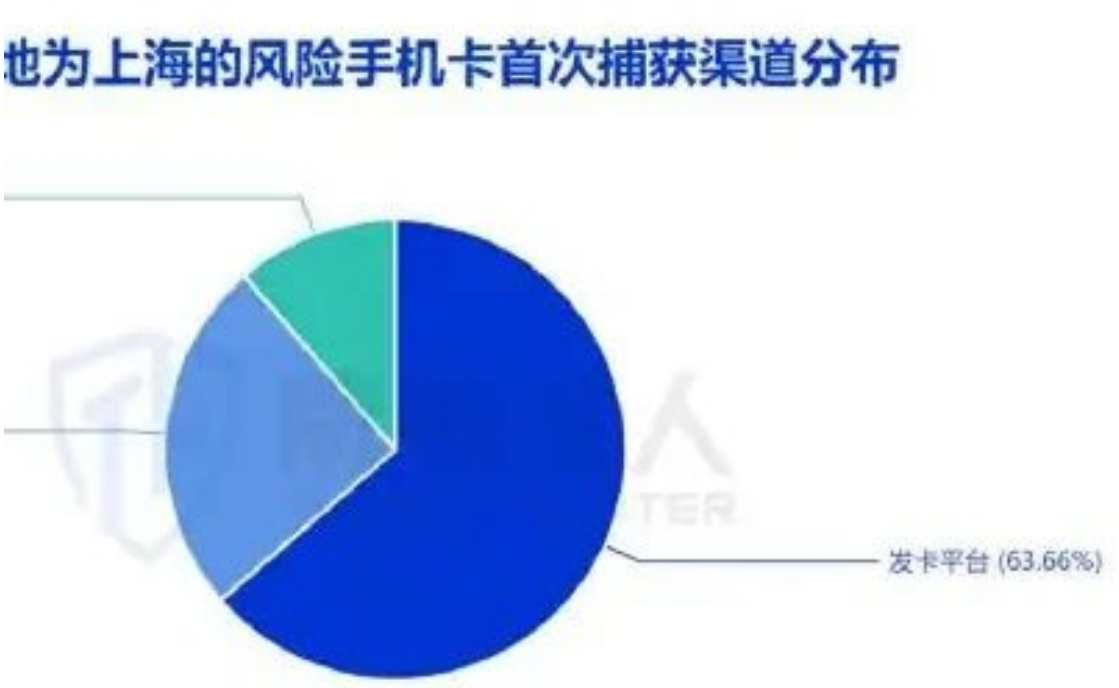
(2) The three provinces with the largest number of new SIM pool cards in the first half of 2024 are: Shanghai, Shandong, and Liaoning. Threat Hunter conducted a statistical analysis of the new domestic SIM pool cards in the first half of 2024 and found that Shanghai, Shandong, and Liaoning (including municipalities directly under the Central Government) are the three provinces with the most SIM pool cards. Analysis of the cities attributable to them found that the three cities with the most SIM pool cards are Shanghai, Chongqing, and Wuhan.

As can be seen from the figure below, the number of new SIM pool cards in Shanghai in the first half of 2024 far exceeded that of other provinces and cities. In-depth analysis found that the main reason was that in March and May 2024, the two leading domestic card issuing platforms held and sold a large number of risky mobile phone cards that were located in Shanghai, and their number accounted for more than 40% of the total new number.

(3) Among the SIM pool cards captured in the first half of 2024, 76.1% belonged to the three major domestic operators. In the first half of 2024, 3.64 million SIM pool cards were monitored, of which 76.1% belonged to the three major domestic operators, and 23.9% belonged to other operators.

2024 Trends in SIM pool card resources in the first half of the year (Chart 1)

Source: Threat Hunter original report, page 13

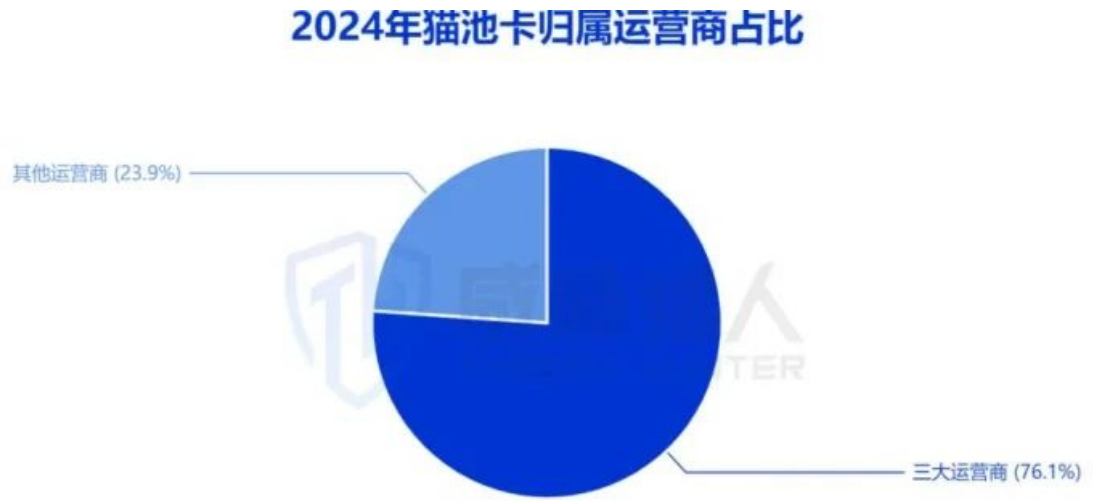


2024 Trends in SIM pool card resources in the first half of the year (Chart 2)

Source: Threat Hunter original report, page 13

2.1.2 Change trend of interception card resources in the first half of 2024

(1) In the first half of 2024, domestic interception cards increased by 42.57% compared with the second half of 2023, and the proportion of interception cards captured for the first time from new channels accounted for as high as 94%. In the first half of 2024, Threat Hunter captured 131,800 new interception cards, an increase of 42.57% from the second half of 2023.



Interception card resource changes in the first half of the year (Chart 1)

Source: Threat Hunter original report, page 14

Interception card resource changes in the first half of the year (Chart 2)

Source: Threat Hunter original report, page 14

Further analysis of the captured interception cards found that there were 6 new interception card source channels in the first half of 2024. Most of the interception cards captured at the same time were captured for the first time by the system, with the first capture accounting for as high as 94%. The increase and rapid update of interception card supply channels undoubtedly increased the difficulty of fraud controls on the business side.

(2) The three provinces with the most interception cards in the first half of 2024 are: Fujian, Guangdong, and Sichuan. Statistical analysis of domestic interception cards captured in the first

half of 2024 found that Fujian, Guangdong, and Sichuan are the three provinces with the most interception cards; in terms of cities, Chongqing, Sanming (Fujian), and Shanghai are the cities with the most interception cards, and there is a large overlap with the cities where SIM pool cards belong.

2024 Interception card resource trends in the first half of the year (figure 1)

Source: Threat Hunter original report, page 15

2024 Interception card resource trends in the first half of the year (figure 2)

Source: Threat Hunter original report, page 15

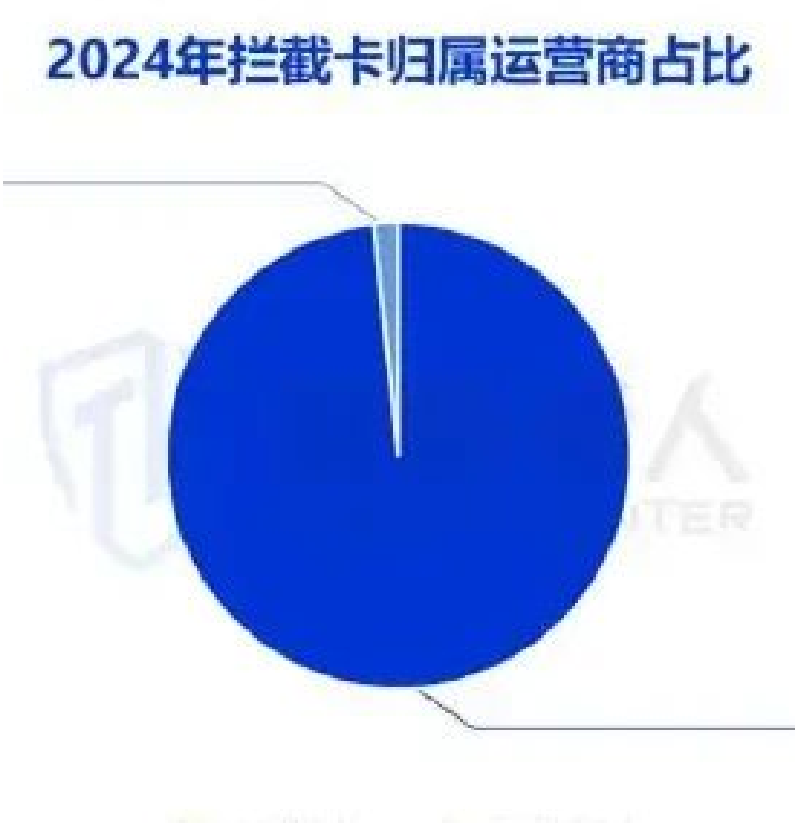
(3) Among the interception cards captured in the first half of 2024, 98.29% belonged to the three major domestic operators. In the first half of 2024, the Threat Hunter intelligence operation platform captured 398,000 interception cards, and the interception cards belonging to the three major domestic operators accounted for 98.31%.

2.1.3 The number of risky mobile phone cards belonging to Hong Kong has increased significantly. In June 2024, nearly 100,000 Hong Kong-related risky mobile phone cards were captured.

Further research on the main source channels of black cards found that in the first half of 2024, the number of risky mobile phone card transactions originating in Hong Kong showed a substantial growth trend. In March 2024, the number of Hong Kong card transactions was only a few thousand, and in June 2024, the number of Hong Kong card transactions reached nearly 100,000.

The number of risk-related mobile phone cards in Hong Kong has increased significantly. From the demand side, from May to June 2024, many online fraud incidents occurred in Hong Kong. During the incident, downstream fraud threat actors used Hong Kong mobile phone cards to register overseas chat software such as Whatsapp to carry out online fraud on the victims. This has led to a substantial increase in the number of Hong Kong cards to a certain extent and also reflects the risk of mobile phones.

Risk trends and supply and demand changes in getting stuck geographically.



There was a significant increase in the number of risk mobile cards attributed to Hong Kong, which captured nearly 100,000 in June 2024.

Source: Threat Hunter original report, page 16

Compared with other domestic mobile phone cards, 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 register Telegram, WhatsApp and other domestic and overseas applications;

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

It can be used repeatedly for several months, while domestic mobile phone cards generally last for several days;

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

4. Supports multiple verification-code reception forms: Hong Kong cards support multiple verification-code reception forms. Currently, Threat Hunter is available on the SMS verification-code receiving service, card issuing website,

Private domain access codes have discovered malicious records of Hong Kong-related mobile phone cards.

2.1.4 Black card material resource labels are more abundant, improving the efficiency of screening threat actors downstream and achieving precise malicious activity.

Threat Hunter research found that in the first half of 2024, threat actors screened and used black card materials in illegal transactions more carefully. Compared with the black card product description field in 2023, in addition to the black card category, registration status and other information provided, the card dealer will also mark the number as "screened", that is, the card dealer will display the historical account information of the number on the order page after purchase, and provide the information.

It is provided to downstream buyers to determine whether it is the target card type, reducing the cost of screening cards and greatly improving the efficiency of downstream threat actors.

或上的风险趋势及供需变化。

The black card resource labels are more abundant, improving the efficiency of the downstream black card and achieving precision.

Source: Threat Hunter original report, page 17

At the same time, Threat Hunter research found that cybercriminal groups can provide accurate account numbers and related information mainly through the cybercrime ecosystem old and new account detection tool. This tool maliciously calls business-related application interface APIs to detect whether the number is registered or has a historical binding record.

2.2 Analysis of risk IP resources in the first half of 2024

The black card resource labels are more abundant, improving the efficiency of the downstream black card and achieving precision.

Source: Threat Hunter original report, page 18

2.2.1 Change trends in risk IP resources in the first half of 2024

Threat Hunter continues to improve its domestic and foreign risk IP monitoring capabilities, providing strong support for Internet platforms to optimize domestic and foreign fraud-control rules. In the first half of 2024, Threat Hunter continued to monitor 55.03 million domestic risk IPs and 102.73 million foreign risk IPs, an increase of 18.62% and 22.44% respectively from the second half of 2023. Our analysis of two types of risk IP, domestic and foreign, found:

(1) The three provinces with the most domestic risk IPs in the first half of 2024: Jiangsu, Guangdong, and Henan (2) The three cities with the most domestic risk IPs in the first half of 2024: Chongqing, Shanghai, and Beijing

(3) The three countries with the most foreign risk IPs in the first half of 2024: Brazil, India, and the United States (4) Among the domestic risk IP types in the first half of 2024, home broadband types account for nearly 90% (5) The overseas risk IP types in the first half of 2024 are mainly home broadband and mobile networks

2024 Risk IP Resource Trends for the first half of the year (Chart 1)

Source: Threat Hunter original report, page 19

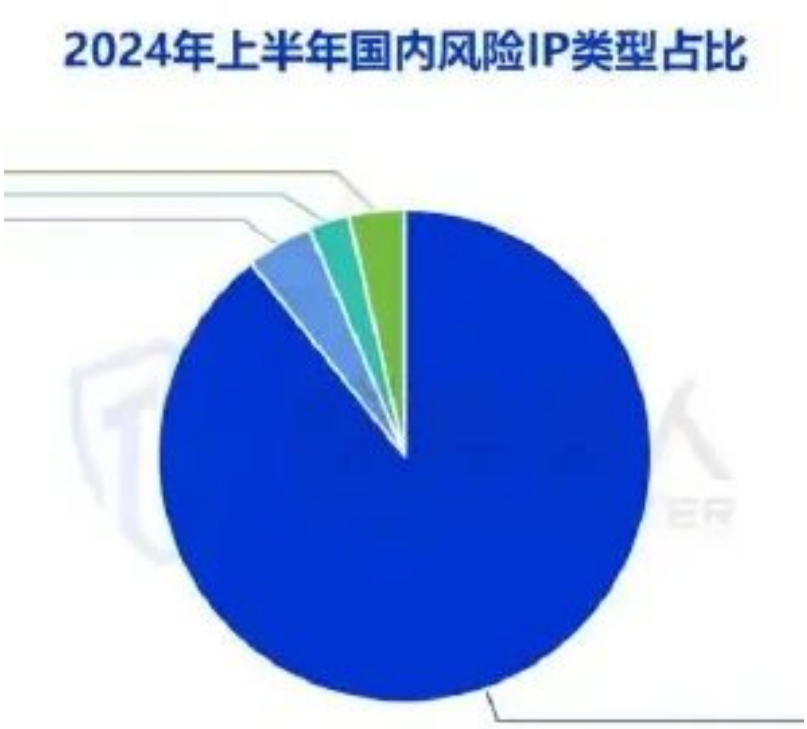
2024 Risks in the first half of the year IP Resource Trends (Chart 2)

Source: Threat Hunter original report, page 19

2.2.2 In the first half of 2024, "hijacking shared proxy" IP attacks accounted for 67% of the total, becoming the main IP type used by attackers

2024 Risk IP Resource Trends for the first half of the year (Chart 1)

Source: Threat Hunter original report, page 20

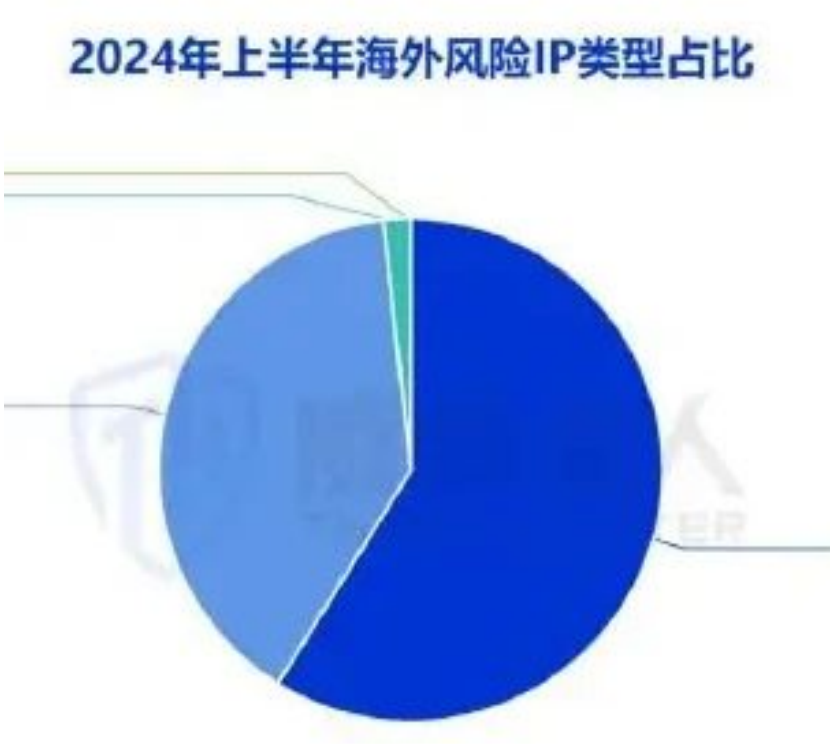


2024 Risks in the first half of the year IP Resource Trends (Chart 2)

Source: Threat Hunter original report, page 20

Threat Hunter continues to monitor the proxy IP platform and found that in the first half of 2024, threat actors' malicious use of normal user IPs by implanting Trojans became more rampant. Judging from the captured data in the first half of 2024, the average daily capture number of "hijacked shared proxy" IPs reached 800,000. The proportion of IP attacks with this label increased from 43.88% (January 2024) to 67.41% (2024) June).

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



2024 In the first half of the first half of the year, the hijacking co-agent IP attacks accounted for 67 per cent of the total and became the main type of IP used by the attackers.

Source: Threat Hunter original report, page 21

2.3 Analysis of online money laundering resources in the first half of 2024

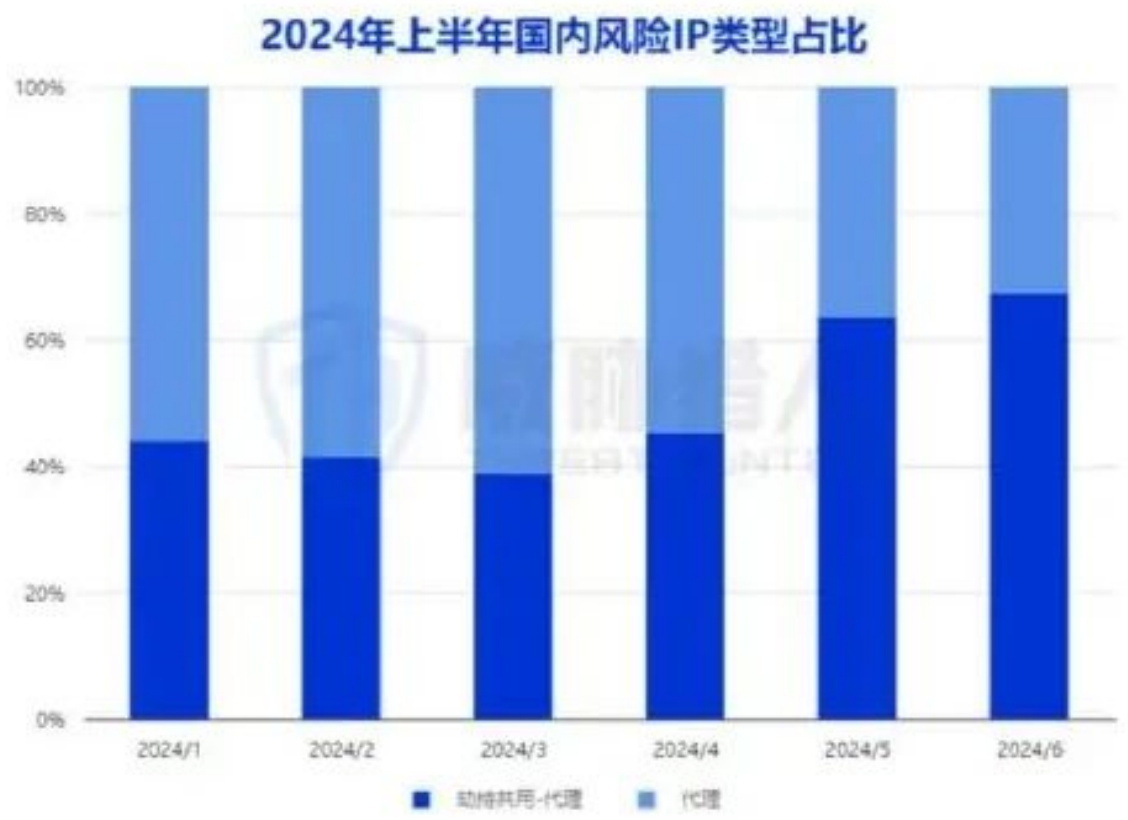
2.3.1 Changes in bank card resources involved in money laundering in the first half of 2024

(1) The number of bank cards involved in money laundering decreased by 28% compared with the second half of 2023, of which the number of benchmark cards dropped by 50.3%. The number of bank cards involved in money laundering in the first half of 2024 was 195,000, a decrease of 28% compared with the second half of 2023. Bank cards involved in money laundering mainly include benchmarking cards, gambling-related cards, and fraud-related cards. Among them, the number of newly added benchmarking cards has dropped the most, down 50.3% from the second half of 2023. Threat Hunter conducted in-depth research on the scoring methods of threat-actor groups and found that in the first half of 2024, the scoring groups gradually switched from benchmarking platforms to Telegaram scores, making monitoring significantly more difficult.

The specific process of gambling platform scoring is as follows:

(2) The proportion of bank cards involved in money laundering belonging to state-owned banks is much higher than that of non-state-owned banks, which is related to the number of cards issued by major state-owned banks.

(3) The main range of bank card money laundering amounts is less than 5,000 yuan. (4) More than 65% of money laundering bank cards are only active on the day of monitoring. Threat Hunter analyzed the "first discovery time" and "latest discovery time" of money laundering bank cards captured in the past six months. It was found that during the statistical period, 65.8% of money laundering bank cards were only active on the day of capture. It can be seen that in order to avoid fraud-control monitoring, fewer bank cards are frequently used for money laundering.

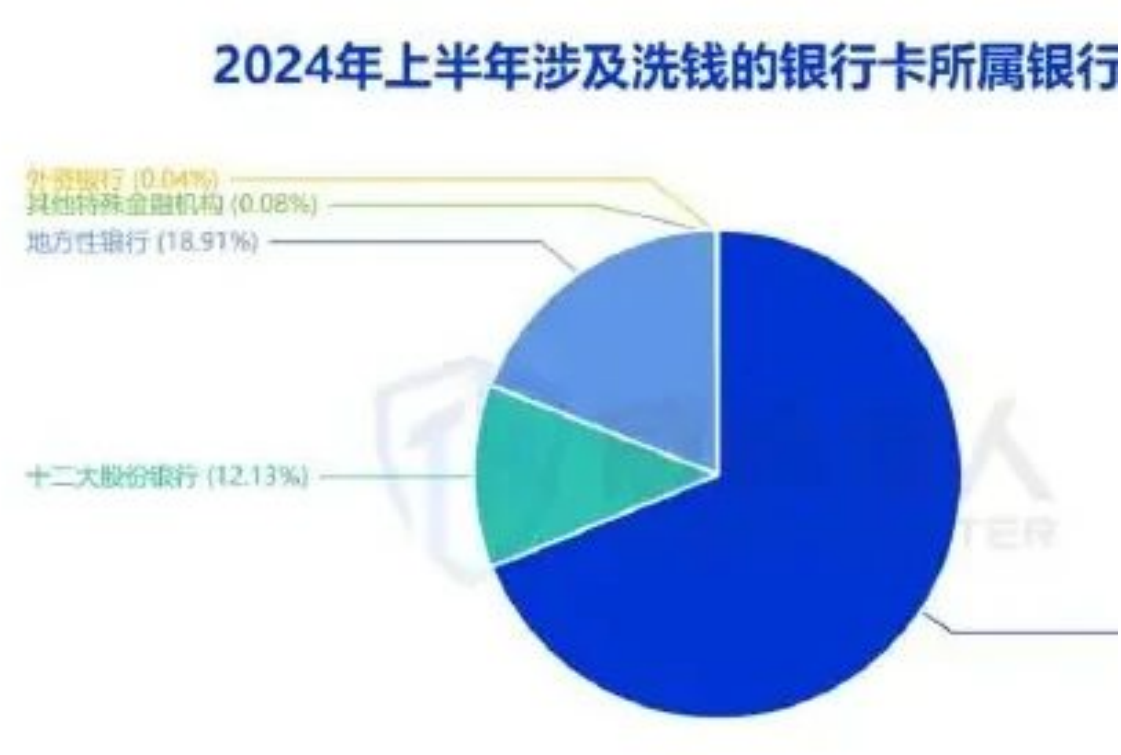


2024 Changes in bank card resources related to money-laundering in the first half of the year

Source: Threat Hunter original report, page 22

2.3.2 Changes in corporate account resources involving money laundering in the first half of 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.



2024 Changes in bank card resources related to money-laundering in the first half of the year (Chart 1)

Source: Threat Hunter original report, page 24

2024 Changes in bank card resources related to money-laundering in the first half of the year (Chart 2)

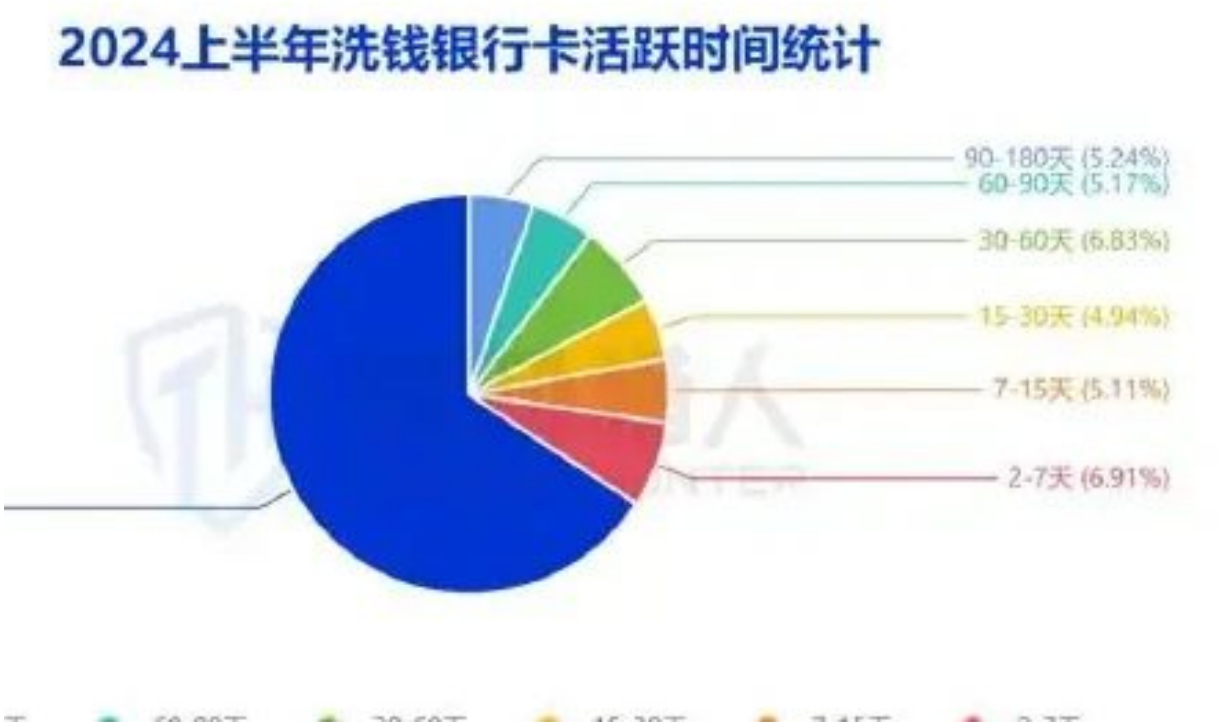
Source: Threat Hunter original report, page 24

(1) The number of public accounts involved in money laundering monitored in the first half of 2024 increased by 16% compared with the second half of 2023. In the first half of 2024, Threat Hunter continued to monitor the bank account resources used by threat actors in the money laundering process and found that the number of public accounts involved in money laundering continued to rise, rising from 3378 to 4386, an increase of 16% from the second half of 2023.

(2) In the first half of 2024, 732 banks were monitored for corporate accounts involved in money laundering, and state-owned banks accounted for 31%. In the first half of 2024, Threat Hunter captured a total of 4,865 corporate accounts involved in money laundering, involving 732 banking institutions. Among the banks with corporate money laundering accounts, state-owned banks accounted for 31.19%.

In addition, the number of corporate accounts of local banks monitored increased by 5.51% compared with the second half of 2023, while the proportion of state-owned enterprises decreased.

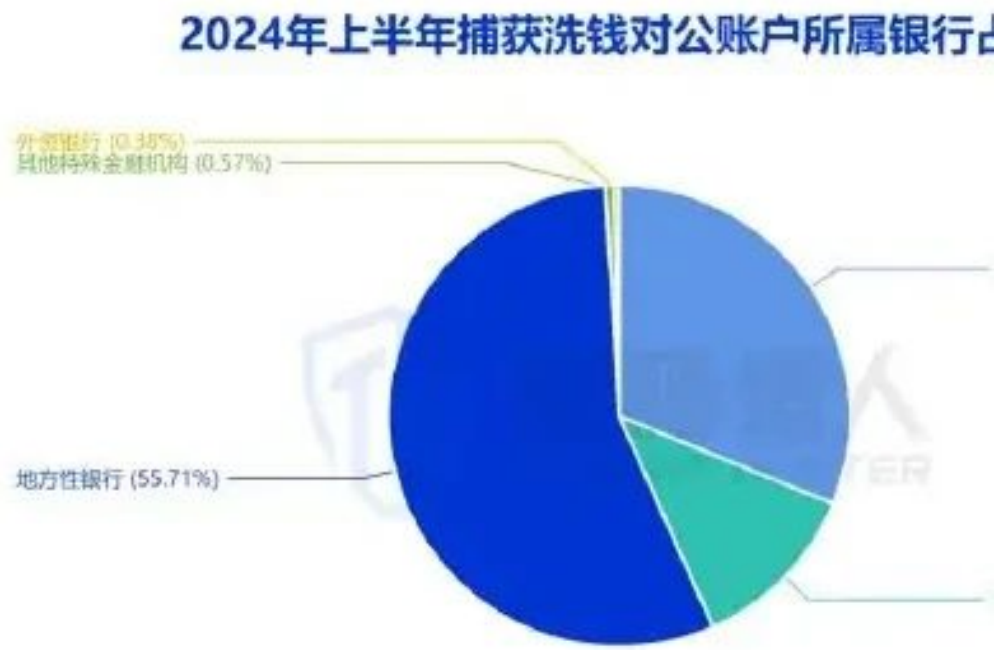
6.06%, in the process of money laundering by threat actors using public accounts, some began to turn to local banks when choosing the bank to open their accounts.



2024 Changes in public account resources in the first half of the year involving money-laundering

Source: Threat Hunter original report, page 25

conduct malicious activity things.



2024 Changes in public account resources in the first half of the year involving money-laundering

Source: Threat Hunter original report, page 26

(3) Among the provinces where public accounts involving money laundering are monitored in the first half of 2024, Anhui, Jiangxi, and Shaanxi entered the top 10 for the first time. The top 5 provinces are basically unchanged from the second half of 2023, while the rankings of Anhui, Jiangxi, and Shaanxi provinces rose to the top 10 for the first time. Ranking, further analysis found that the growth trend of corporate accounts of local banks in such provinces is obvious. Behind this change in rankings, to a certain extent, it also reflects the trend of money laundering gangs gradually using rural credit cooperatives and corporate accounts of local banks.

2.3.3 In the first half of 2024, pornographic fraud and money laundering funds accounted for more than 70% of the total amount

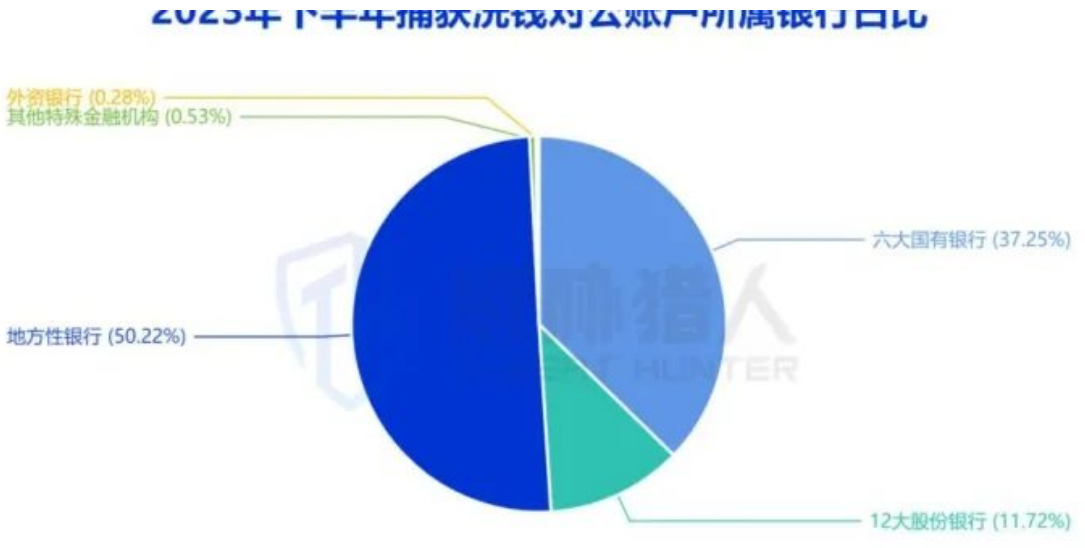


Table 1

Source: Threat Hunter original report, page 27

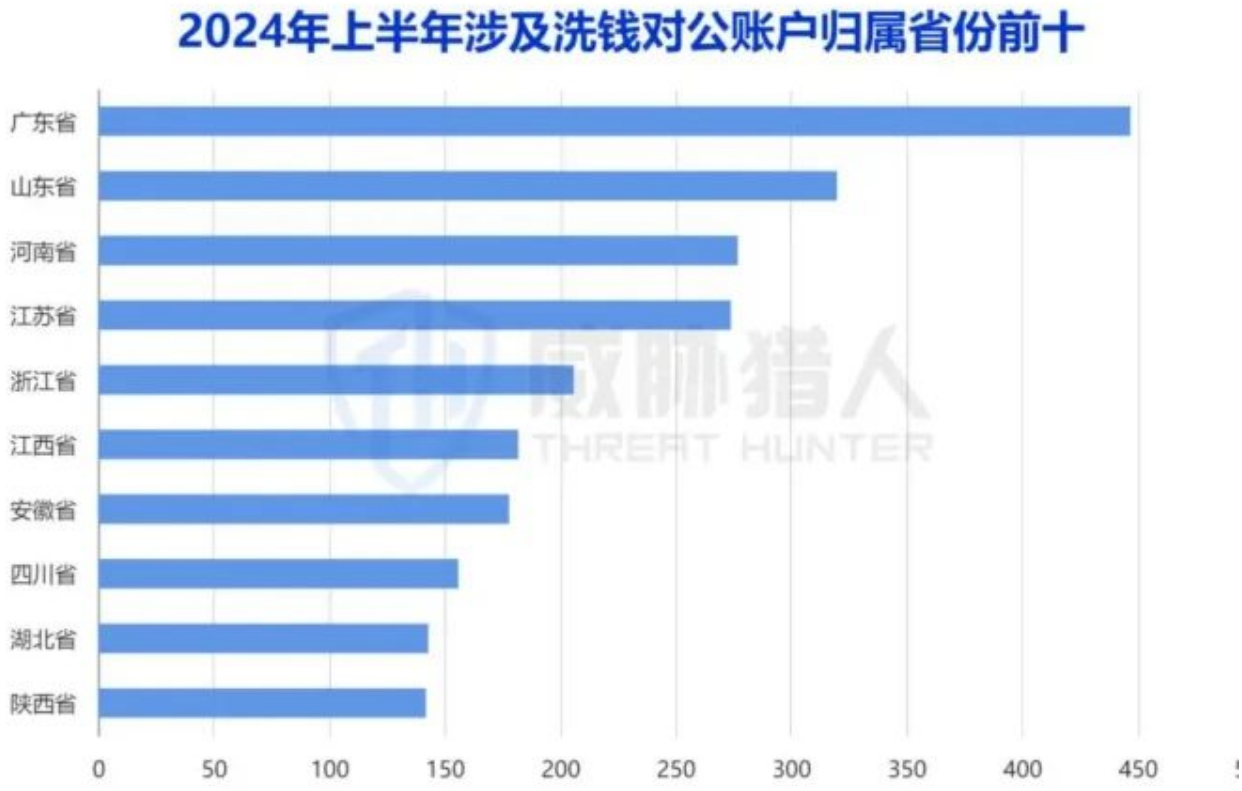


Table 2

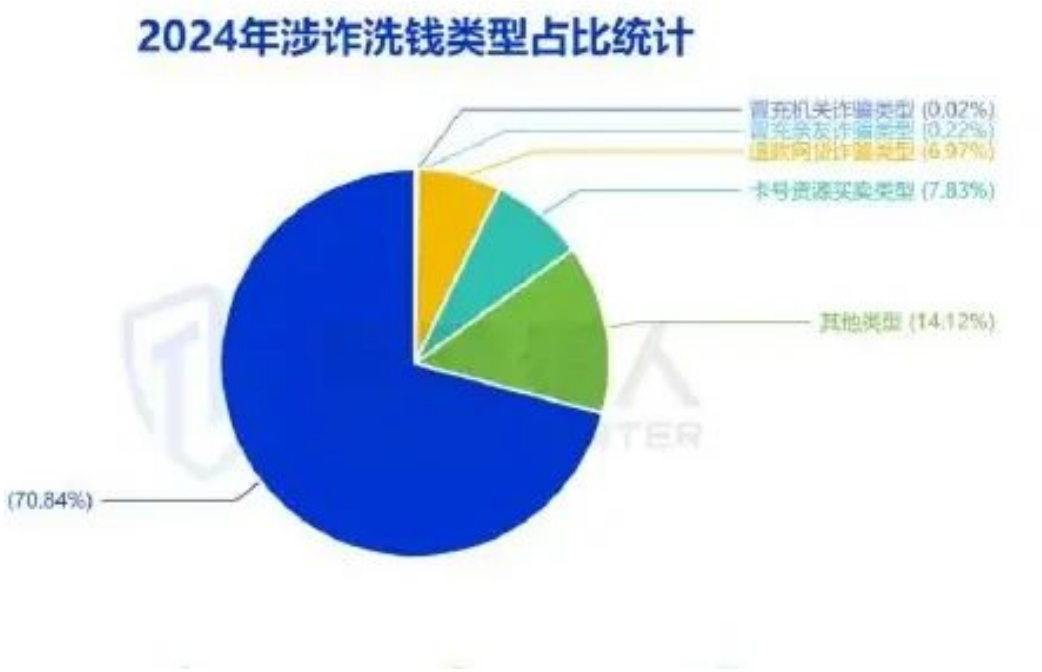
Source: Threat Hunter original report, page 27

Based on the amount of fraud committed by threat actors and the degree of risk, the currently monitored fraud techniques of threat actors can be roughly divided into 6 types, among which pornographic fraud is the most common type, accounting for more than 70%. According to research and investigation, it is found that fraud forms such as impersonating government agencies, impersonating relatives and friends, and refund online loan fraud have higher risks and larger fraud amounts. Pornographic bill fraud has relatively lower risks and smaller fraud amounts, generally less than 5,000 yuan.

Pornography fraud: It mainly refers to fraud that induces victims to complete designated fraud tasks by publishing false information through pornographic websites, text messages, dating software, etc.

Card number resource trading fraud: mainly refers to fraud that assists threat actors in money laundering by selling or renting card numbers. The risk mainly depends on the purpose of threat actors.

2.4 Analysis of risk mailbox resources in the first half of 2024



2024 Fraudulent money-laundering in the first half of the year in the form of sexual billing was over 70%

Source: Threat Hunter original report, page 28

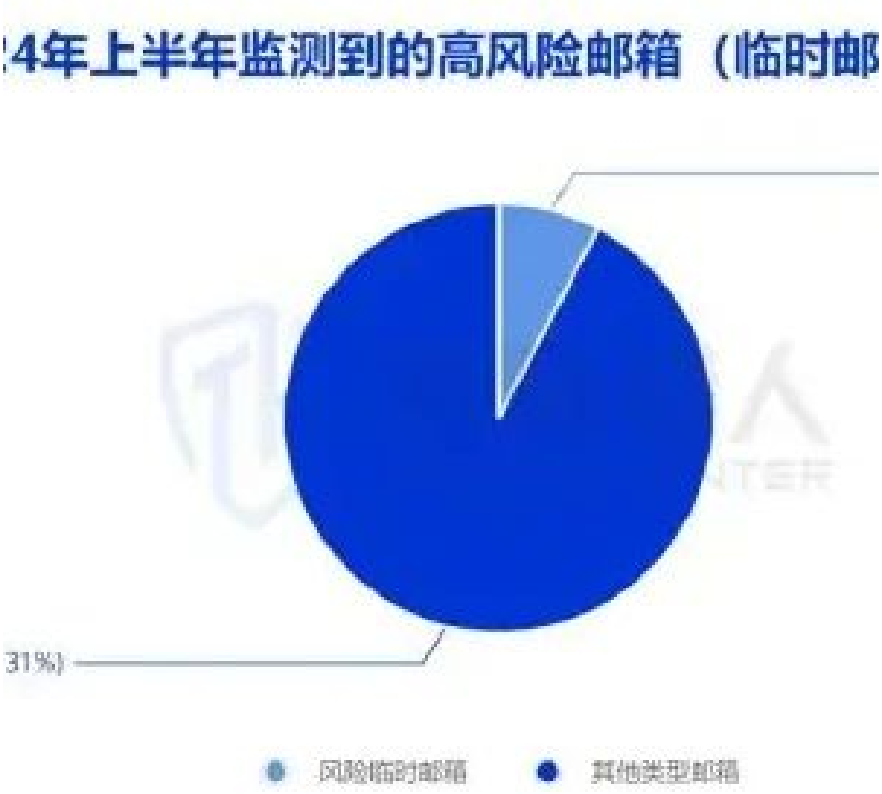
2.4.1 Changes in risk mailbox resources in the first half of 2024

(1) Monitoring and identification of high-risk mailboxes (temporary mailboxes) in the first half of 2024 accounted for 7.69% of the total. Judging from the number of monthly monitoring and identification of different types of risk mailboxes in the first half of 2024, 35,666 risk mailboxes were identified in the first half of 2024, of which more than 84% were identified as low-risk corporate mailboxes, and high-risk mailboxes (temporary mailboxes) accounted for

7. 69%, the new mailboxes are mainly concentrated in corporate mailboxes.

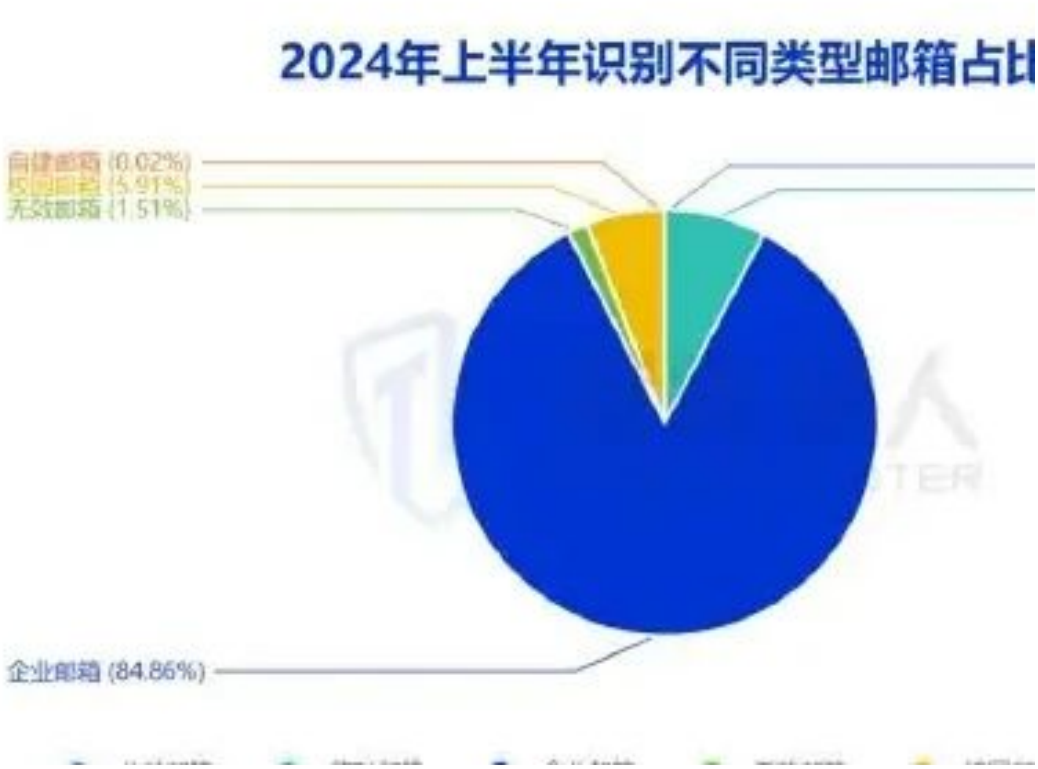
(2) In the first half of 2024, more than 98.15% of the number of email domain names came from the Top 10 websites that provide free temporary email services. In terms of risky email addresses, in the first half of 2024, we monitored and found 8,804 temporary email domain names, and the Top 10 websites that provided free temporary email services contributed more than 98.15% of the number of email domain names.

Analysis of common attack techniques by threat actors in the first half of 2024



2024 Changes in risk mailbox resources in the first half of the year (Chart 1)

Source: Threat Hunter original report, page 29

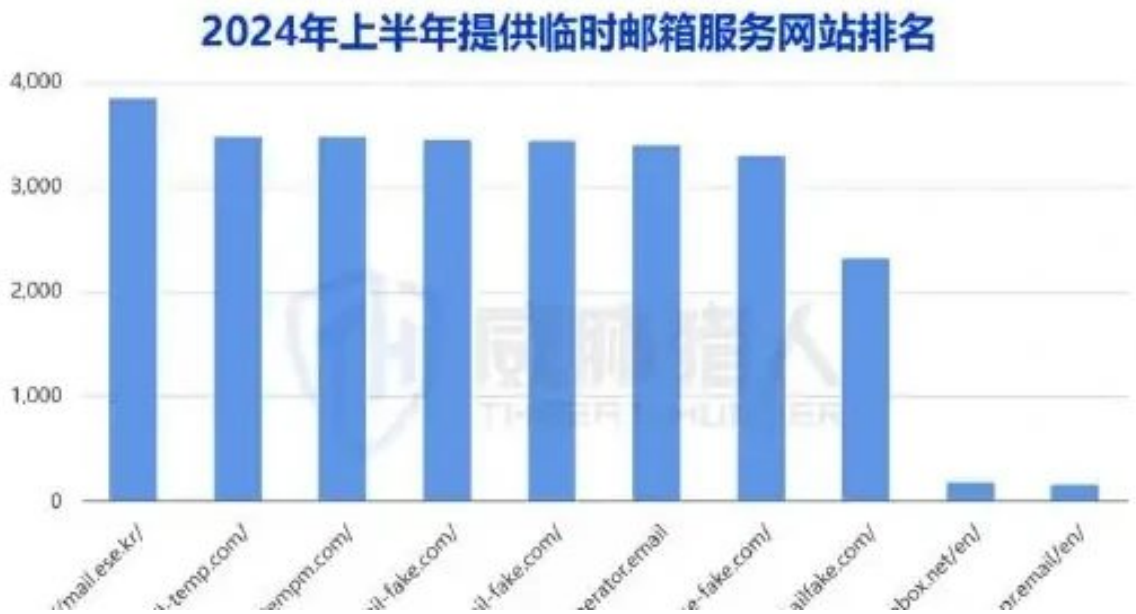


2024 Changes in risk mailbox resources during the first half of the year (Chart 2)

Source: Threat Hunter original report, page 29

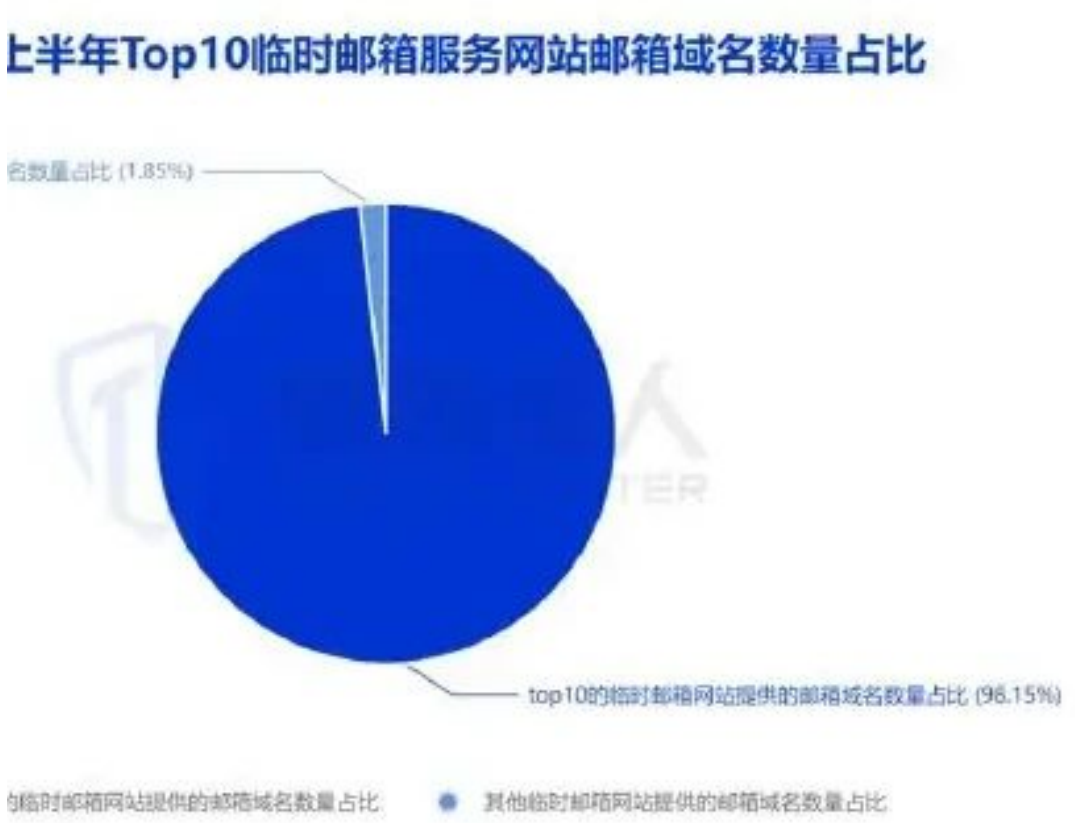
3. Analysis of common attack technologies by threat actors in the first half of 2024

3.1 threat actors use LSPatch technology to quickly grab orders and conduct malicious activity, and are frequently used in platform apps such as finance, social networking, and real estate.



2024 Changes in risk mailbox resources in the first half of the year (Chart 1)

Source: Threat Hunter original report, page 30



2024 Changes in risk mailbox resources during the first half of the year (Chart 2)

Source: Threat Hunter original report, page 30

Threat Hunter research found that in the first half of 2024, many threat actors used a technical tool called "LSPatch" to "quickly grab orders" to conduct malicious activity. At the same time, apps in many industries such as finance, social networking, real estate, and local life discovered malicious behaviors that used LSPatch technology to quickly grab orders.

LSPatch is essentially a technology that uses Hook framework modules without Root. With this technology, users can use Hook framework modules on non-Root mobile phones to implement hook mobile phone system functions and modify the overall execution logic of the functions. Through this tool, threat actors package the specific malicious environment and tools into the attacked app, allowing users to directly install the fake app injected with malicious tools to quickly grab orders, which greatly reduces the user's tool usage threshold.

In the traditional Xposed or Lsposed framework, users usually need to obtain root permissions to install and use various modules to achieve personalized customization and system optimization of mobile phone applications. For users who are not familiar with technology, this process not only has a high operating threshold, but also risks "bricking the phone". The emergence of Lspatch has undoubtedly opened a new door for such users. Users can easily experience the powerful functions brought by the Xposed module without root permissions.

Taking the local life app as an example, threat actors use LSPatch technology to embed a hook module in the takeout order app, so that the app has the function of automatically grabbing orders. A delivery boy only needs to purchase the "takeout order app" from threat actors and install it normally to automatically grab orders. The order threshold and cost of the takeaway boy are

greatly reduced. The comparison between order grabbing tools using LSPatch technology and previous order grabbing tools is as follows:

3.2 threat actors use HID devices to carry out automated attacks, making their crimes more covert and making monitoring more difficult.

Threat Hunter research found that in addition to automated script tools such as Key Wizard and auto.js pro, threat actors will use HID devices to conduct automated operations attacks more frequently in the first half of 2024. With the development of technology, most HID devices have developed

It has begun to support Bluetooth protocol for transmission, allowing threat actors to achieve simple sliding click operations through "HID device + Bluetooth protocol". Among them, the scenario that attracts the most attention from threat actors is the "short video traffic manipulation" scenario.

HID (Human Interface Device) is a commonly used device type in USB devices. It is a USB device that directly interacts with people. Devices such as keyboards and mice are the most common HID devices in daily life. Since HID devices have no obvious characteristics at the software level, attacks using such devices are more stealthy.

Take the short video volume-boosting scenario as an example. The first step in short-video volume-boosting is to maintain an account, and account maintenance requires the account to continuously watch a certain type of video, allowing the platform's recommendation algorithm to complete labeling of the account. In order to achieve automated clicks in short video sales while trying to bypass platform fraud controls, in addition to automating clicks based on mobile developer permissions and phone root permissions, there are also many threat actors who "automate clicks based on HID devices."

Take the "Automated Clicking Based on HID Device" tool recently analyzed by Threat Hunter as an example. The main operating process is as follows:

The method of "automatic clicking based on HID devices" controls the hardware through code, and the hardware sends HID instructions to implement specific click activity operations. It is different from the current mainstream automated click implementation methods based on code and ADB operating device clicks; and this method does not require the configuration of a specific environment (such as developer permissions, root environment), which makes the existing automated click fraud-control rules of most platforms potentially ineffective in identifying this method, further increasing the platform's detection costs.

Analysis of threat actors attack scenarios in the first half of 2024

4. Analysis of threat actors attack scenarios in the first half of 2024

4.1 Marketing fraud scenario analysis

4.1.1 Marketing activities

(1) 4.08 million pieces of marketing campaign attack intelligence, involving 8,000 groups of malicious threat actors. In the first half of 2024, Threat Hunter captured a total of 4.08 million pieces of marketing campaign attack intelligence, monitored 8,000 active malicious social groups, and involved 65,000 malicious threat actors. Overall, this was a decrease compared to the second half of 2023. The decline in intelligence volume in February was mainly affected by the slowdown in transactions by threat actors during the Spring Festival. The volume of attack intelligence gradually picked up after the holiday.

(2) A large number of threat actors maliciously pay compensation for special products on e-commerce platforms. Some threat actors said that "one compensation order is enough for half a year." With the rapid development of e-commerce platforms, many e-commerce platforms have effectively improved platform traffic and competitiveness through loose return rules such as customer returns without reason. This rule has been discovered and exploited by threat actors invisibly, and the cybercrime ecosystem group that uses platform rules to make malicious compensation continues to grow.

In April 2024, the Threat Hunter intelligence platform detected a large number of attacks by threat actors known as "super rights defenders". In January, there were only sporadic threat actor advertisements, and the number of discussions increased to nearly 200 in April. In-depth digging revealed that many threat actors have attracted more groups of threat actors to launch attacks on e-commerce platforms and related merchants with high compensation such as "one order can last for half a year." Incidents of malicious compensation and attacks in the name of "rights protection and anti-counterfeiting" continue to emerge.

Different from the past conventional compensation ideas such as "three noes", "anti-counterfeiting", and "non-delivery", "super rights protection" refers to the cybercrime ecosystem targeting "poisonous and harmful" goods for sale on the platform, conducting drug testing and issuing reports, filing administrative reconsiderations, administrative lawsuits, letters and visits, threatening merchants to enter negotiation and mediation for compensation, and even finally obtaining court enforcement funds. The compensation process involves the country's public authorities, the overall review cycle is long, and the time required for small, medium and large compensation varies.

In order to successfully obtain compensation, compensation threat actors said that they have a supply team, a receiving inspection team, a legal team, etc. to accompany them throughout the process to recruit users who are willing to pay the principal and "boarding fee" to teach compensation. This is also the upgrade of the "super rights protection" compensation gameplay.

The main product types include: tadalafil (sexual dysfunction drugs), sibutramine (weight loss), and ephedrine (weight loss). They are basically drugs that require a prescription from a doctor or have ingredients prohibited by the State Food and Drug Administration. If included in the product, it constitutes a violation of the law.

Marketing activities (Chart 1)

Source: Threat Hunter original report, page 36

Marketing activities (Chart 2)

Source: Threat Hunter original report, page 36

The main compensation process is as follows:

(3) threat actors use the "lock order" method to join forces with users to cash out bank deposits, and the division of labor for malicious purposes acts has become more refined. In recent years, incidents of platform users and cybercrime ecosystem jointly cashing out platform preferential activities have occurred frequently. Users receive their rights normally.

After receiving the rights, the cybercriminal group cashes out and distributes the realized profits with the users in proportion, reducing the additional cost of the threat actors gang looking for cash buyers or "forced consumption". This joint cash-out further reflects the efficient use of resources and the refined division of labor for malicious purposes acts.

Many banking institutions launch monthly or weekly payment discount activities. This type of activity has always been a gold-mining project that the cybercrime ecosystem and promotion-abuse actors pay close attention to. In the large-amount instant discount activities of designated banks, the highly collaborative behavior of cybercriminal groups and bank users to cash out and share profits has become more rampant. The technique of locking orders after payment to obtain discounts has gradually been widely used on e-commerce platforms.

Marketing activities

Source: Threat Hunter original report, page 37

In the first half of 2024, Threat Hunter monitored a large number of threat actors taking advantage of loopholes in bank payment rules to jointly cash out with users through "locking discounts", "locking orders", etc. The specific processes and techniques are as follows:

1. Place an order with a merchant who can easily get instant bank discounts, and deliberately enter the wrong password during the payment stage to lock the discount quota;

2. Purchase products that can be refunded at any time (such as tickets or hotels) to lock in the discount of this order, and you will retain the immediate discount qualification for the month after refund;

Marketing activities

Source: Threat Hunter original report, page 38

3. In the cash-out stage, the user provides the payment code to the threat actors, and the threat actors withdraw the bank's immediate deduction, and the threat actors return the payment amount and part.

The methods of separately reducing funds, sharing profits with users, and jointly locking orders with users give threat actors sufficient time to cash out their attacks.

For example: after a user locks an order with "20 coupons off for spending over 100", he shows the payment code to threat actors. The threat actors use relevant qualifications to scan the code and deduct 100 yuan for the "order". The user finally pays 80 yuan, and the threat actors get 100 yuan, and privately return 90 yuan to the user. Through this cash-out method, threat actors and the user each get a 10 yuan instant discount, and the bank loses 20 yuan. Yuan Li reduces the equity.

4.1.2 Content flushing

(1) There are 510,000 pieces of content traffic manipulation fraud information, and there are 3,977 malicious groups involved in traffic manipulation. In the first half of 2024, the situation of traffic manipulation fraud is still severe. During this period, the Threat Hunter security team monitored a total of 510,000 pieces of traffic manipulation fraud intelligence involving live broadcast platforms, content platforms, e-commerce platforms, and application download platforms. In addition, 3,977 active social groups involved in traffic manipulation were detected, and the number of people participating in these threat actors' activities reached 9,014.

(2) Over 75% of content platforms and live streaming platforms suffered from traffic manipulation attacks, and human-operated fraud and traffic manipulation is still the mainstream method. Threat Hunter continuously monitors the traffic manipulation intelligence released by each platform and found that in the first half of 2024, content platforms and live broadcast platforms suffered the most serious traffic manipulation attacks, with traffic manipulation-related malicious information accounting for more than 75% of the total. This is mainly reflected in content platform views, comments and sharing traffic manipulation, live broadcast platform popularity interactions, rankings, and gift traffic manipulation.

From the perspective of traffic manipulation methods, human-operated fraud is still the mainstream traffic manipulation method. Threat Hunter has monitored that human-operated fraud-related intelligence accounts for 74% of the total traffic manipulation intelligence. As major platforms continue to update their identification technologies for malicious traffic manipulation behavior, many traffic manipulation studios have shifted from using protocol traffic manipulation and group control traffic manipulation based on real devices to using human-operated traffic manipulation to further meet the platform's requirements for real and effective traffic. This change reflects the platform's effective crackdown on technical means for traffic manipulation.

(3) The application of new methods of increasing volume in live broadcast rooms such as "natural flow traffic manipulation" has become more common. With the rapid development of digital media, live streaming has become an important model of commercial sales. Problems such as difficult to predict effects and unstable traffic have caused problems for many live broadcast merchants. Due to the high price of paid streaming on the platform, threat actor groups have begun to focus on the business opportunities of natural traffic traffic manipulation.

The recommendation mechanism of natural traffic on the live broadcast platform means that only users with specific tags who enter the live broadcast room and perform likes and comments and other traffic-boosting behaviors will become high-quality traffic, so more refined human-operated traffic-boosting methods have emerged.

Natural traffic, also known as "recommended feed flow", refers to the content information flow that is continuously updated and presented to users. The types of natural traffic in live broadcast rooms include but are not limited to:

1. Traffic to the Live Broadcast Square: Through fans’ likes in the live broadcast room and setting attractive covers and titles, traffic can be diverted from the Live Broadcast Square.

flow;

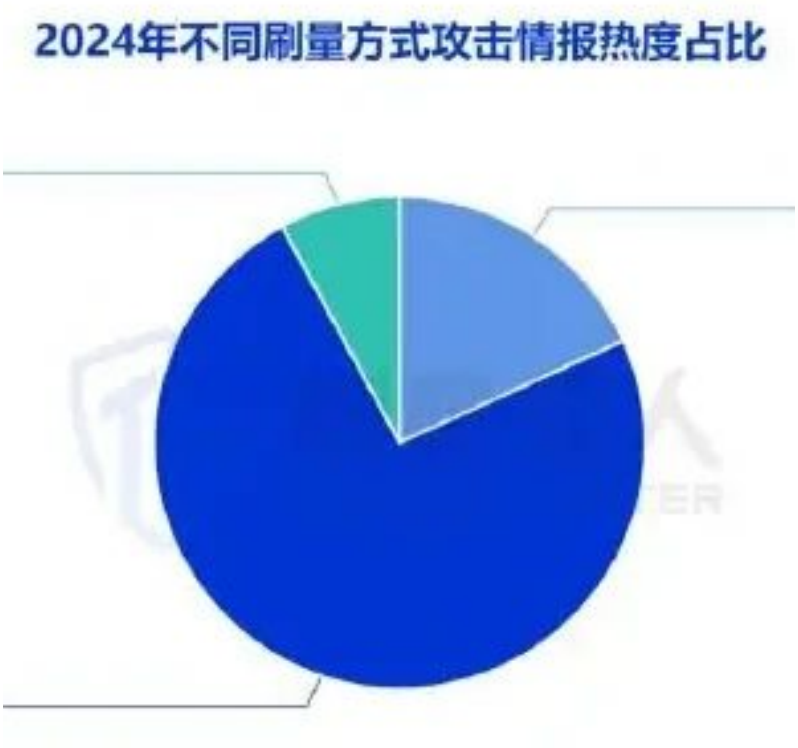
2. Same-city traffic: Use the same-city positioning function and turn on the same-city positioning when the broadcast starts to attract people in the same city to view your live broadcast;

3. Search traffic: Traffic through personal homepage, search, order center and other sources, although it does not account for a large proportion, it is also a natural recommendation

A type of referral traffic.

Content brush (Chart 1)

Source: Threat Hunter original report, page 41



Content brush (Chart 2)

Source: Threat Hunter original report, page 41

In the first half of 2024, Threat Hunter observed that the application of new natural flow volume traffic manipulation techniques such as "live broadcast square traffic manipulation" became more common.

Taking "live broadcast square traffic manipulation" as an example, in order to effectively increase the popularity of the live broadcast room and make it a recommended traffic for the live broadcast square, threat actors use a large number of mobile phone accounts and cloud control software to manipulate the live broadcast room. Specific behaviors include:

1. "Maintain accounts" in advance: maintain accounts in advance, use the same type of content to simulate the target user group, so that subsequent accounts can be directly

The traffic recommendation between broadcast rooms is more accurate;

2. Push the stream to the live broadcast square: By controlling a large number of accounts, follow the main account and watch short videos for more than 20 minutes, and then use

The live broadcast room is pushed to the live broadcast square to obtain greater traffic;

3. Enter the designated live broadcast room to further increase the volume: Use the cloud control software again to batch control mobile phone accounts, enter the designated live broadcast room to further increase the volume.

Perform a series of operations such as following, liking, commenting, and lighting up signs to further enhance the authenticity and activity of live broadcast traffic.

Under the operation of the cloud control software, hundreds or even thousands of accounts instantly flooded into the designated live broadcast room. The live broadcast room that was originally unattended suddenly surged in popularity, attracting more "wild" traffic. The entire process "prejudged" the system's push of user preferences, but in fact most of it was fake traffic.

This type of traffic manipulation method has a cumbersome process and high cost. Threat Hunter conducted in-depth research and learned that a single account of this type of traffic manipulation method that simulates natural traffic can cost more than 5 yuan, which is at least twice the price of an ordinary human-operated traffic manipulation account. This also reflects the growing demand for "real traffic" in the live broadcast industry. At the same time, the platform's fraud controls of various traffic manipulation techniques is increasing.

4.2 Analysis of financial fraud scenarios

(1) In the first half of 2024, there were 460,000 pieces of credit fraud attack intelligence, and 2,700 active malicious activity groups were monitored. In the first half of 2024, Threat Hunter captured a total of 460,000 pieces of credit fraud attack intelligence, and monitored 2,700 active malicious activity social groups, involving 14,000 malicious activity threat actors.

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

From the perspective of geographical distribution, the top five regions with the hottest credit fraud in the banking industry in the first half of 2024 are: Shandong, Zhejiang, Hebei, Chongqing, and Beijing.

(2) Forging and packaging false identities such as "business owners" to carry out debt fraud, and the forgery techniques are more abundant and lifelike. Debtors are often those with clean credit records and in urgent need of large amounts of funds but without the ability to repay. By falsely packaging these people's personal assets and other information, they can obtain high-value loans from banks and obtain profits of tens or even millions. The price paid is to abandon their credit records and face legal sanctions. In July 2024, the number of dishonest enforcers in China reached 8.33 million, including a large number of professional debtors.

Due to the frequent occurrence of debt risk incidents, banks and other financial institutions have attached great importance to it, and the fraud controls policies for debt fraud and loan fraud have become more stringent. In order to maximize profits and avoid being cracked down by relevant agencies and legal authorities, relevant threat actors have made the identity packaging and material forgery of debtors more realistic, using methods that are close to "real" to increase the success rate of fraudulent loans.

In order to avoid bank fraud controls and ensure maximization of interests, threat actors intermediaries will package various false identities for debtors such as "workers, household heads, business owners" as conditions for credit enhancement when applying for loans. Specific methods include real payment of social security and provident funds to debtors, transfer of real estate/business, real invoicing and tax payment, real leasing business scenarios, etc.

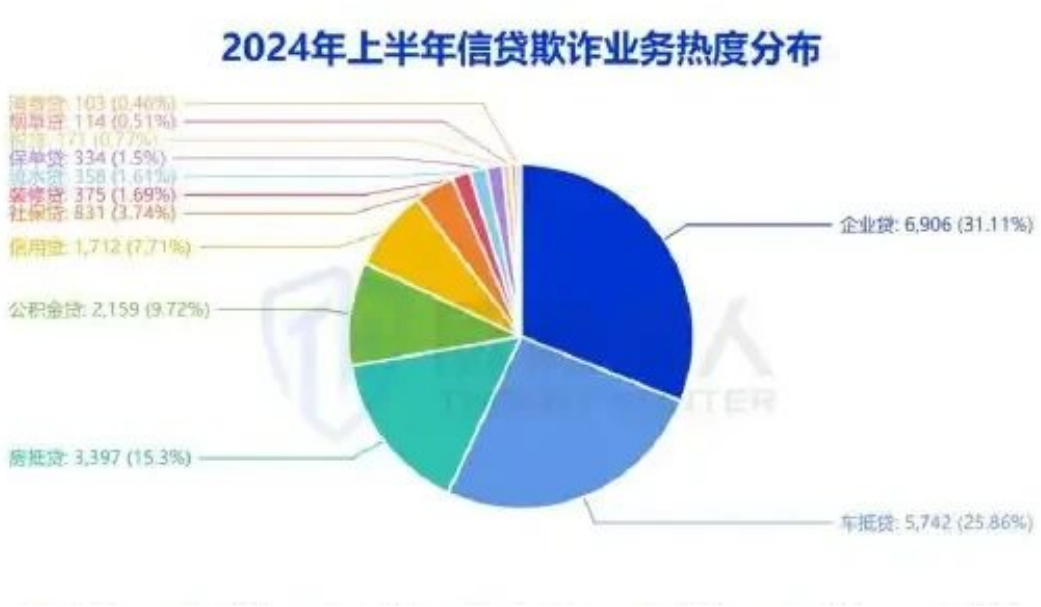
Through a series of packaging preparations, threat actors will use the various qualifications of the debtor to carry out one-stop large-amount financing of "house loans, credit loans, corporate loans, and car loans." It is understood that the total amount of fraudulent loans by a debtor ranges from 5 to 20 million yuan, and the actual amount received is 40%-60% of the total debt. After the loan is

successful, in order to avoid being discovered and labeled as a fraud, many threat actors do not hesitate to increase the cost of fraudulent loans and help/instruct the debtor to repay the loan for half a year or even two years.

The specific process of threat actors operating debt-taking and loan fraud is as follows:

(3) The fraudulent business of non-standard loans has been active in the first half of 2024, and the popularity of non-standard loan-related topics has increased by nearly 10%. Non-standard loans: refers to the fact that customers cannot meet the standard conditions for conventional loans, and threat actors use packaging materials, beautified data, and relationships to defraud loans.

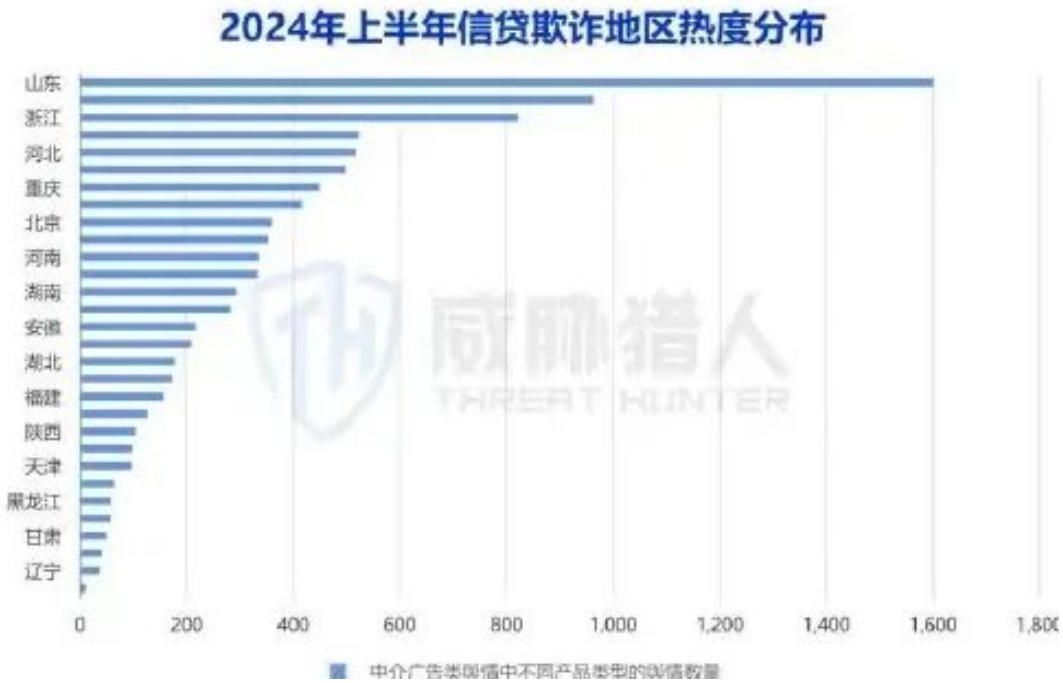
贷、房抵贷、公积金贷和信用贷。



Financial fraud scenario analysis (Chart 1)

Source: Threat Hunter original report, page 45

、重庆、北京。



Financial fraud scenario analysis (figure 2)

Source: Threat Hunter original report, page 45

In the second half of 2023, the number of discussions on non-standard related topics reached 140,780. In the first half of 2024, the total popularity of non-standard topics was 154,685, with a growth rate of 9.9%.

Under the influence of the economic downturn in recent years, enterprises, operators, and individuals have generally faced difficulties such as reduced income and high debt, making the existing qualifications of some enterprises, operators, and individuals unable to meet the loan requirements of financial institutions. threat actors and intermediaries commit fraud through false flow sheets (individuals and enterprises), technology quota increases, car financing cash out, fake renovation loan cash out, rent-to-purchase cash out, etc., and use false materials and false demands to pass the approval and quota increase system, making non-standard businesses continue to be active.

4.3 Analysis of telecom network fraud scenarios

(1) In the first half of 2024, there were 290,000 pieces of telecom fraud attack intelligence, and 10,187 active malicious activity groups were detected. In the first half of 2024, the Threat Hunter risk intelligence platform detected 290,000 pieces of telecommunications fraud-related intelligence, 10,187 active malicious activity social groups, and 17,000 malicious activity threat actors.

(2) Frauds using the "screen sharing" function of various remote conferencing software are frequent. In the first half of 2024, fraud incidents using the "screen sharing" function of remote conferencing software occurred frequently. Fraudsters obtain passengers' personal and related

business information through some illegal channels, pretend to be employees of airlines, insurance agencies, etc., and use some specific words (such as "refund", "claim settlement", "book change", etc.) to induce the victim to install remote conferencing software and turn on the "screen sharing" function, thereby obtaining the victim's SMS verification code, or even payment password, etc., and finally successfully steal the victim's bank card, or successfully induce the victim to transfer money to a designated account. The specific process is as follows:

Give a real case:

Li received a call from an unknown person, pretending to be the "customer service" of an airline, telling him that his flight needed to be changed and compensation would be provided, and asked him to click on an online meeting link to start screen sharing. Since the other party could accurately tell his flight information, Li believed it and performed screen sharing in accordance with his request.

At this time, the scammer took advantage of this function to obtain Li's personal information, and asked Li to provide his bank card number, password, mobile phone verification code and other information on the pretext of identity authentication and unbinding his bank card, and performed facial recognition. In the end, all 30,000 yuan in Li's bank card was transferred away by the other party.

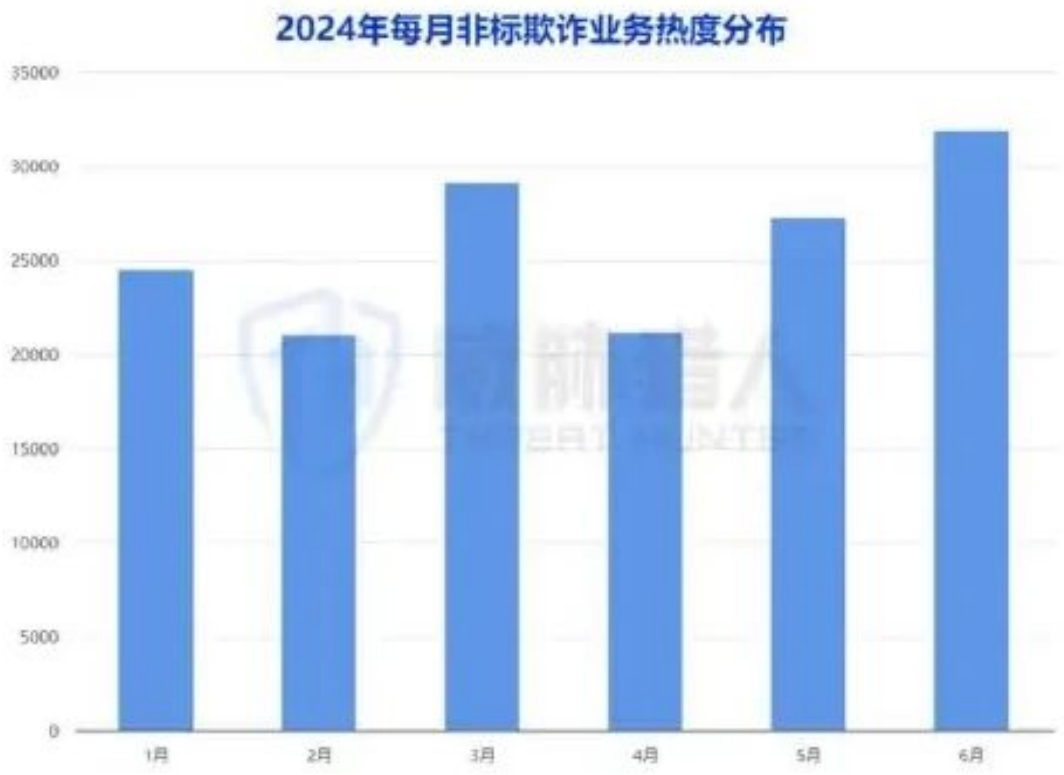
The following is a summary of remote conference names mined from electronic fraud scenarios:

(3) threat actors develop various types of remote control software and forge them into commonly used apps, which greatly increases the success rate of fraud. In the process of fish killing scams, fraud gangs will induce victims to install remote control software (such as ready.apk). threat actors disguise such software as normal apps (such as anti-fraud center app, etc.) to gain the trust of the victim and make them feel at ease.

Enable barrier-free service authorization, thereby controlling the victim's mobile phone and collecting mobile phone information, remotely controlling the mobile phone to transfer money, successfully stealing the victim's bank card, or successfully inducing the victim to transfer money to a designated account.

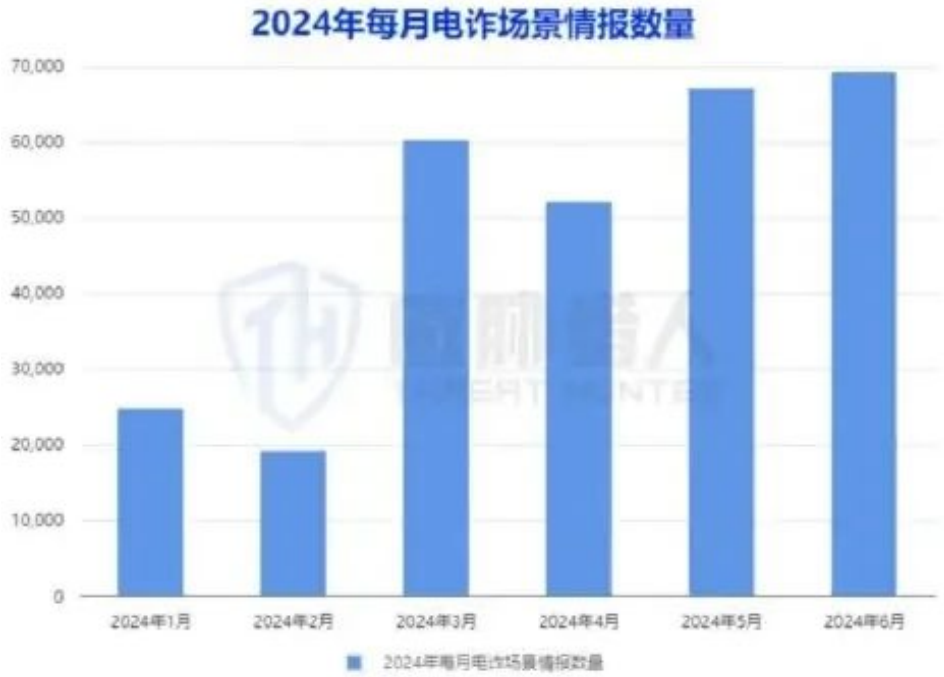
By counterfeiting "remote control" apps of various daily applications, threat actors control victims' mobile phones in the background, making many victims completely undetectable and difficult to defend against, which greatly increases the success rate of threat actors' fraud. In March 2024, Zhang from Lianyungang met a stranger while playing the mobile game Peace Elite at home and offered skin as a gift. He controlled his phone through the "ToDesk" app and recharged an unknown game account through mobile banking for a 648 yuan Peace Elite package 7 times, resulting in a loss of 4,536 yuan.

In order to induce victims to download and install remote control software, threat actors gangs will design different techniques and words according to different groups of people and psychological characteristics. Victims often complete the download without warning and get "rewards" and fall into the scam.



telecommunication network fraud scenario analysis (Chart 1)

Source: Threat Hunter original report, page 48



Telecommunication network fraud scenario analysis (figure 2)

Source: Threat Hunter original report, page 48

Some promotional words are as follows:

telecommunication network fraud scenario analysis (Chart 1)

Source: Threat Hunter original report, page 49

Telecommunication network fraud scenario analysis (figure 2)

Source: Threat Hunter original report, page 49

4.4 Analysis of Phishing and Counterfeiting Scenarios

(1) In the first half of 2024, 33,453 phishing and counterfeiting-related incidents were monitored, involving 243 companies. In the first half of 2024, Threat Hunter monitored a total of 33,453 cases of phishing websites and counterfeit apps, involving 243 companies, which was an 8.97% decrease from the total number of monitoring in the second half of 2023, and the overall growth trend was maintained. Such websites and apps are counterfeited

Normal websites and apps gain users' trust and defraud users of their personal information and money.

(2) The top three industries most severely affected by phishing and counterfeiting: e-commerce, securities, and consumer finance. Judging from the industry distribution data in the first half of the year, the top three industries for phishing website counterfeiting are e-commerce, the securities industry, and the consumer finance industry. Among them, the e-commerce industry surpassed the financial industry and became the industry most severely affected by phishing and counterfeiting attacks. Counterfeiting cases in the e-commerce industry accounted for more than 50% of the total.

Research on counterfeiting data related to the e-commerce industry found that there are three main characteristics:

1. Counterfeit websites in the e-commerce industry usually appear in the form of counterfeit shopping mall platforms;

2. Counterfeit e-commerce platforms generally have 1-4 types of counterfeit templates, which completely imitate the necessary web pages and

The app download interface, customer service system and mall management backend, the counterfeiting effect is very realistic;

3. cybercriminal groups tend to register the same counterfeit website in batches to conduct malicious activity, casting a wide net while bypassing fraud controls to the greatest extent possible. Lord

This should be reflected in the fact that generally the second-level domain name and URL path of the counterfeit website set by threat actors are consistent, and the domain name registration time is basically the same.

(3) Investment fraud occurs frequently, mainly counterfeiting "securities" industry websites. During the economic downturn, many people want to make quick profits in the short term through effective investment. threat actors take advantage of this group of people's desire for short-term gains to commit investment fraud. Investment fraud mainly attacks the financial industry, among which counterfeit securities industry websites are the most common.

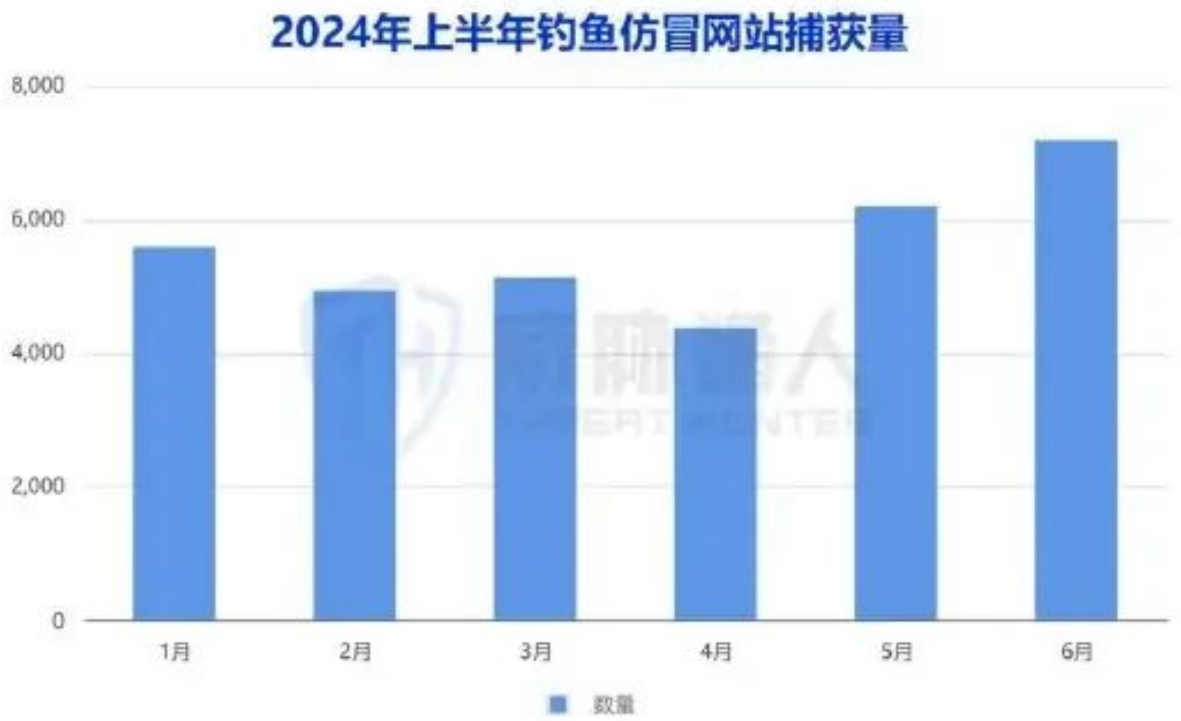
Investment plate: Mainly refers to counterfeit websites or app "investment plates" that target financial industry companies with strong counterfeit investment attributes. The main process and role division are as follows:

Upstream threat actors build counterfeit websites: threat actors generally purchase the source code of counterfeit websites on the source code platform and arrange for developers to deploy the environment for counterfeiting the target website;

Upstream "investment managers" attract traffic and acquire customers: by purchasing target group data, or through mainstream social platforms and short video platforms

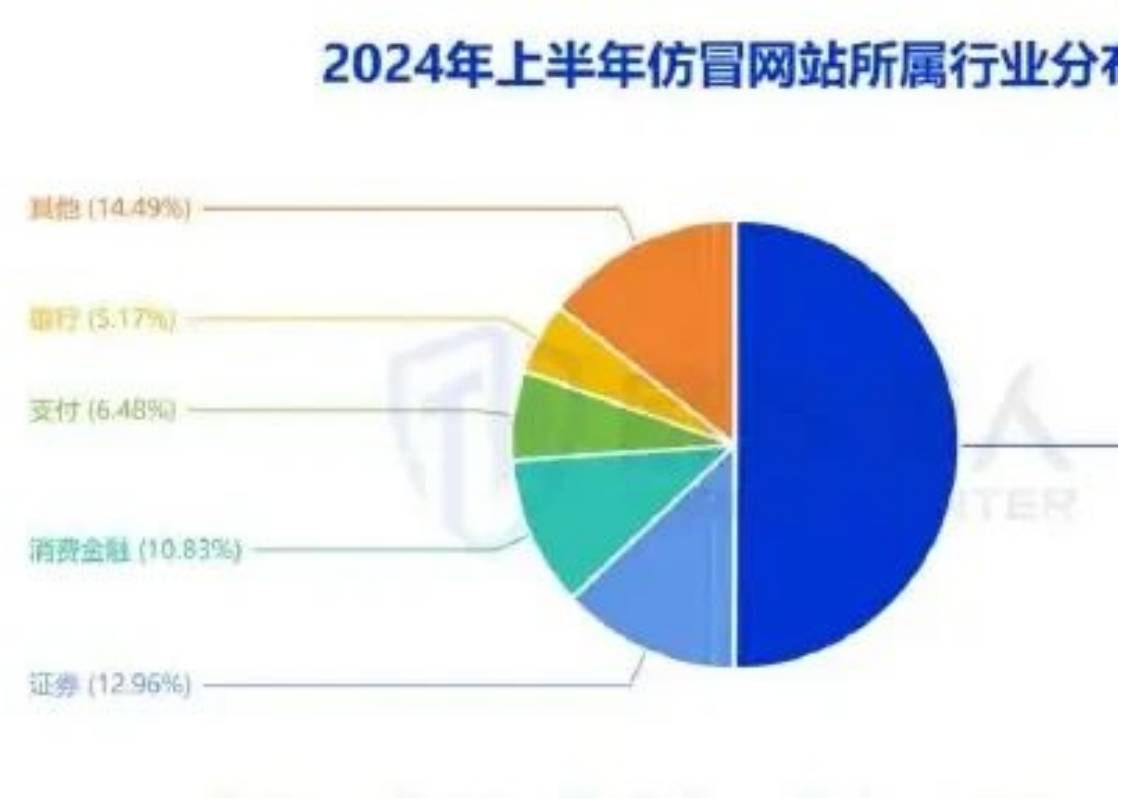
Carry out traffic acquisition and customer acquisition;

Midstream "managers" contact target customers: contact target users with words such as a company's feedback to customers, introduction of financial products, event invitations, etc. "Managers" generally create elite profiles on social software to enhance credibility and reduce victims' defensiveness.



Fake scenario analysis for fishing (Chart 1)

Source: Threat Hunter original report, page 52



Fake scenario analysis for fishing (Chart 2)

Source: Threat Hunter original report, page 52

Downstream "investment platform customer service personnel commit fraud: that is, people who conduct fraudulent operations. Counterfeit websites in the securities industry usually involve operations such as capital investment and cash withdrawals."

In the "investment market", threat actors usually set specific rules, such as setting the initial capital investment to 100,000 yuan and the closing fund to 500,000 yuan. Before the market is closed, users can perform operations at the market at will, such as investing, withdrawing cash, etc., to further gain users' trust. When the user's investment reaches 500,000 yuan, threat actors will cancel the user's withdrawal and run away.

4.5 Analysis of Brand Advertising Fraud Scenarios

(1) Among brand advertisers who have suffered fraud, the food and beverage category has become the largest advertiser to suffer from advertising fraud. Threat Hunter has captured a large amount of advertising fraud data based on advertising traffic monitoring, involving multiple industries, and the food and beverage category has become the advertiser to suffer from the largest proportion of fraud.

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

(2) Judging from the forms of fraudulent advertisements, the proportion of fraudulent advertisements that have been played 100% reaches 78%. Judging from the forms of fraudulent advertisements in the captured data, 15-second video advertisements are the mainstay of

fraudulent advertisements, and this type of advertisements accounts for more than 99% of the total amount of fraudulent advertisements captured.

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 78%. This data is obviously not in line with the behavior of normal users. In reality, there are not many users who 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) Terminal situation of forged brand advertisements In the fraud link of advertising fraud, the reported fraudulent advertising traffic often contains dynamically changing forged 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:

The fake mobile terminals of advertisements include mobile phones and tablets, mainly mobile phones, covering the following mobile phone brands:

The counterfeit Internet smart terminals in the advertisement include smart TVs, TV boxes, smart screens, smart speakers (with screens), singing machines, projectors and other smart terminal brands:

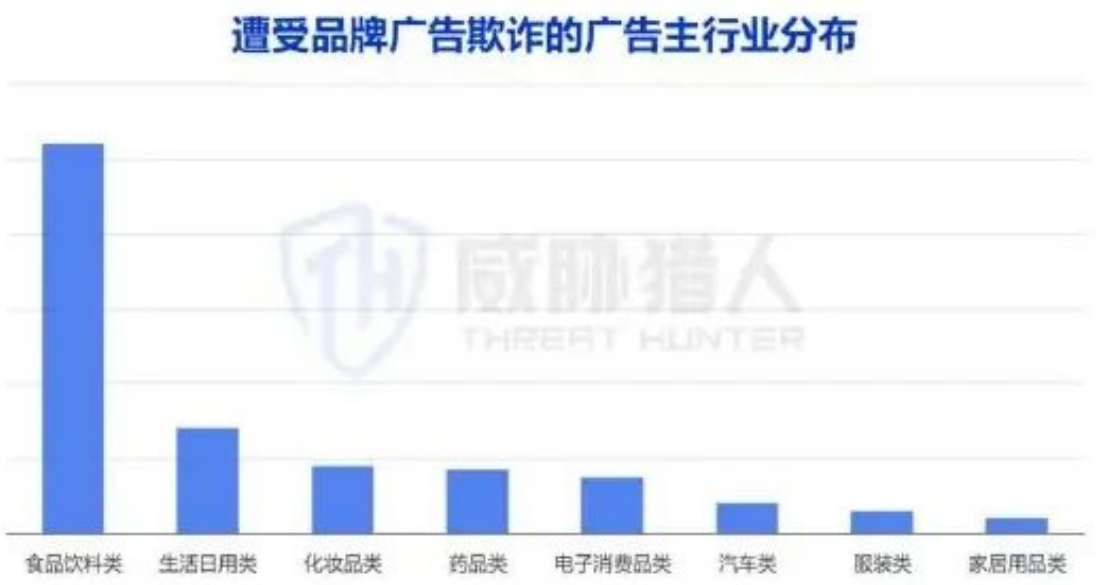
4.6 Data leakage scenario analysis

(1) There were a total of 16,011 data breaches in the first half of 2024, an increase of 59.58% from the second half of 2023. According to data from the Threat Hunter data leakage risk monitoring platform, among the 110 million pieces of intelligence monitored across the entire network in the first half of 2024 (January to June), there were a total of 16,011 valid data breaches based on the authenticity verification engine and DRRC manual analysis, an increase of 59.58% from the second half of 2023. In the second half of the year, it increased by 59.58% to 9,539.

Threat Hunter found that the number of data breaches dropped significantly in February 2024, down 36% from January 2024 (898 cases). Further analysis revealed that it was mainly due to the following two aspects:

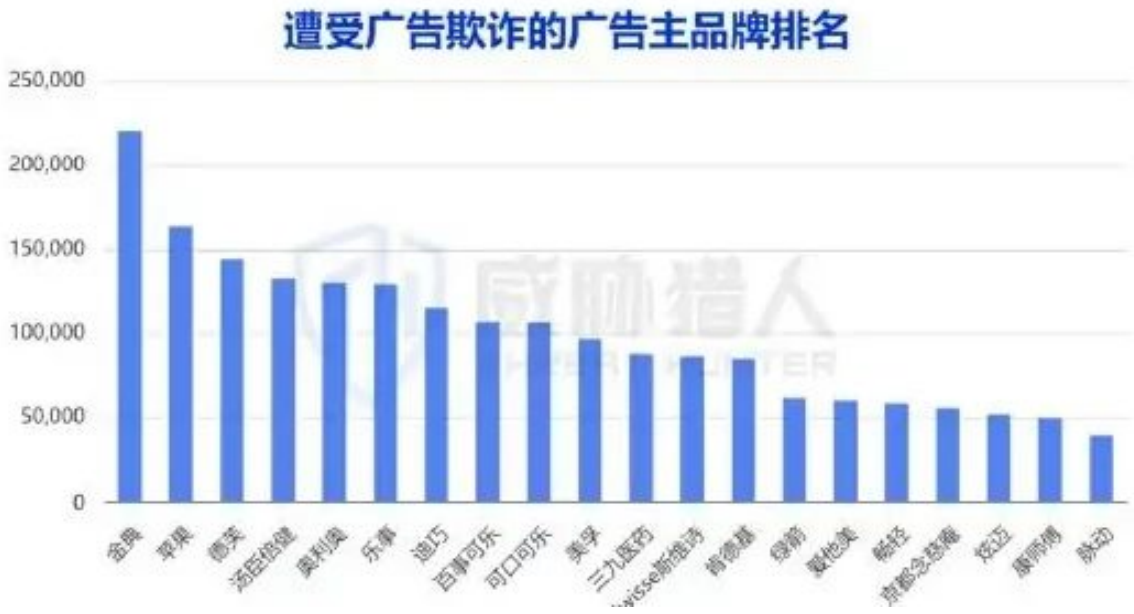
From the perspective of the source of data leakage, the number of data leakage incidents caused by different reasons such as third-party leakage and SMS channel leakage all declined in February 2024. It can be seen that it was mainly affected by the slowdown in trading behavior caused by the holiday of threat actors during the Spring Festival.

Judging from the number of threat actor groups that sell data (middlemen), the number of illegal data trading threat-actor groups dropped in February 2024.



Analysis of brand advertising fraud scenarios (Chart 1)

Source: Threat Hunter original report, page 55



Analysis of brand advertising fraud scenarios (Chart 2)

Source: Threat Hunter original report, page 55

(2) Banking, e-commerce, and consumer finance have become the top three industries with the number of data breach incidents, with 2,961 banking incidents ranking first. From the perspective of industry distribution, data breach incidents in the first half of 2024 involved 85 industries and 1,524 companies. The top five industries with the number of data breach incidents are banking,

e-commerce, consumer finance, insurance, and express delivery. Among them, data breaches in the banking industry

The number of incidents reached 2,961, making it the industry with the largest number of data breach incidents.

The changes in the rankings of the top 10 industries in the first half of 2024 are as follows:

The top industries for data leakage are mainly the finance and e-commerce industries. Data leakage incidents in the financial industry are mainly reflected in the reselling of customer information by banks, consumer finance, insurance and other companies. They are usually used by downstream threat actor groups for targeted marketing and fraud. Because they involve a large amount of high-value user data and are close to the transaction link, they have become the hardest hit area for personal information leakage.

Analysis of brand advertising fraud scenarios

Source: Threat Hunter original report, page 56

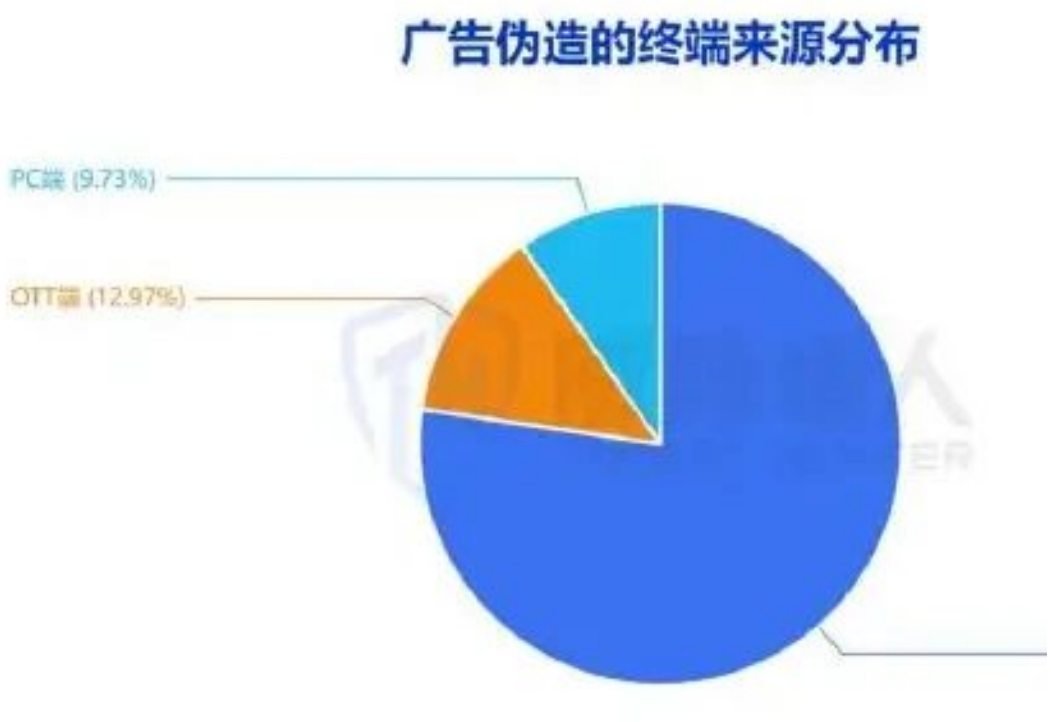
In recent years, online shopping has developed even more vigorously. According to the "Statistical Report on China's Internet Development" released in March 2024, as of December 2023, the number of online shopping users in China reached 915 million, accounting for 83.8% of the total Internet users.

With the continued and steady growth of online shopping, e-commerce platforms have generated a massive amount of shopping orders and logistics information. Due to their large exposure, these shopping orders and logistics information have become key targets of threat actor groups and are also used for marketing or fraud.

At the same time, among the "Top Ten Most Frequent Types of Telecom Network Fraud" recently announced by the Ministry of Public Security, 10 common types of telecom network fraud, such as fraudulent bill rebates, fake online investment and financial management, fake shopping services, fake reseller logistics customer service, and fake credit reporting, accounted for nearly 88.4% of the cases.

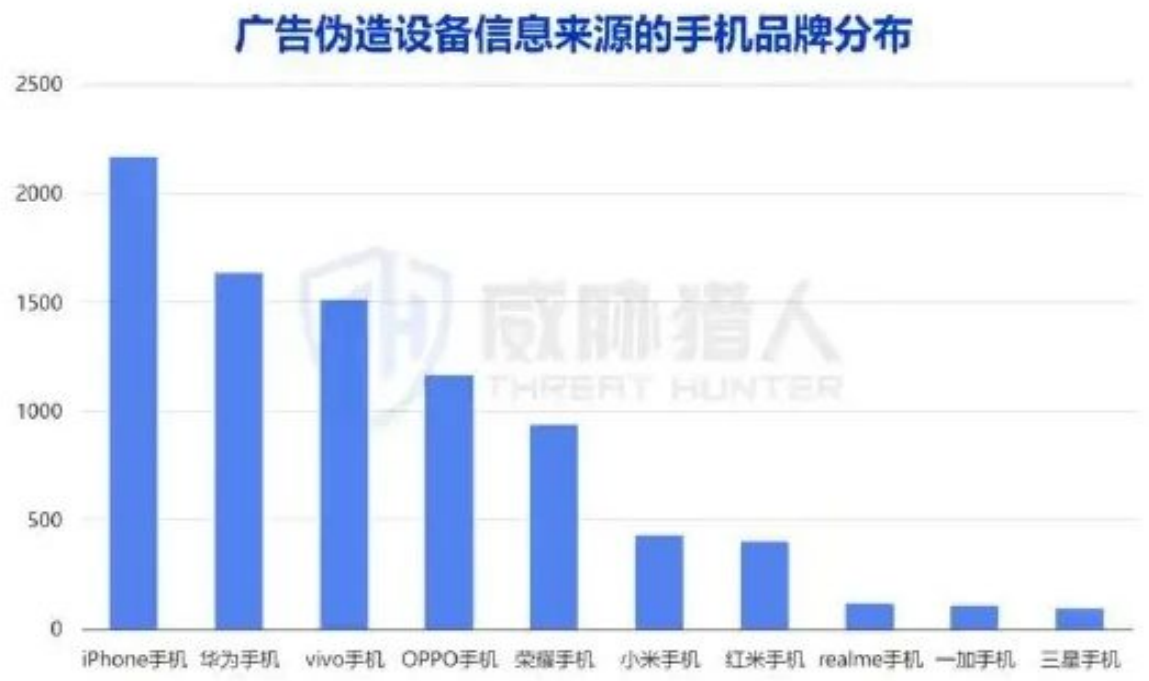
Among them, rebate fraud is the type of fraud with the largest number of cases and the most losses. Fake online investment and financial management fraud cases have the largest losses. The number of cases of fake shopping service fraud has increased significantly and ranks third. Financial and e-commerce user groups are the victims of such fraud cases.

(3) In the first half of 2024, there were many fraud activities using Facetime, and there were a total of 1,237 risk events related to the "iOS" field, an increase of 8 times compared with the second half of 2023. Threat Hunter security researchers found that in the data leaked in the first half of 2024, the frequency of the "device information" field information gradually increased, especially the "iOS" type data fields, which were trafficked underground. Judging from the chat records between the actors group and downstream data buyers, the data buyers mentioned the screening requirements for "iOS" device data many times in their data repurchase requirements.



Analysis of brand advertising fraud scenarios (Chart 1)

Source: Threat Hunter original report, page 57



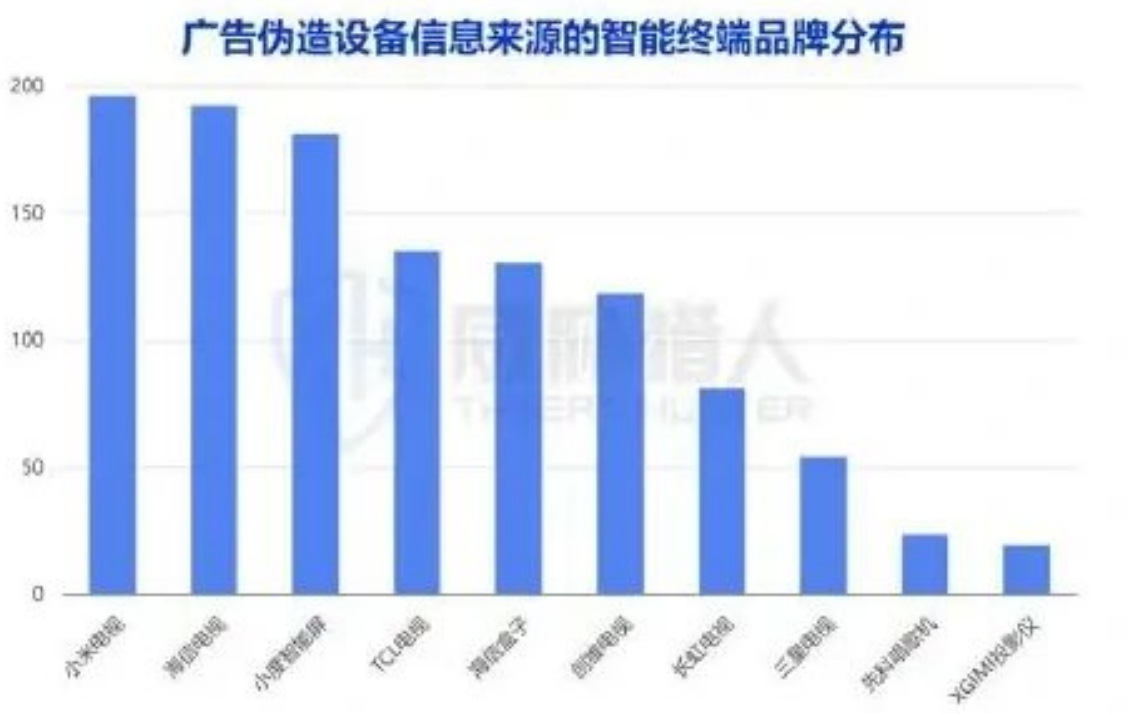
Analysis of brand advertising fraud scenarios (Chart 2)

Source: Threat Hunter original report, page 57

(The leaked data captured by Threat Hunter contains device information)

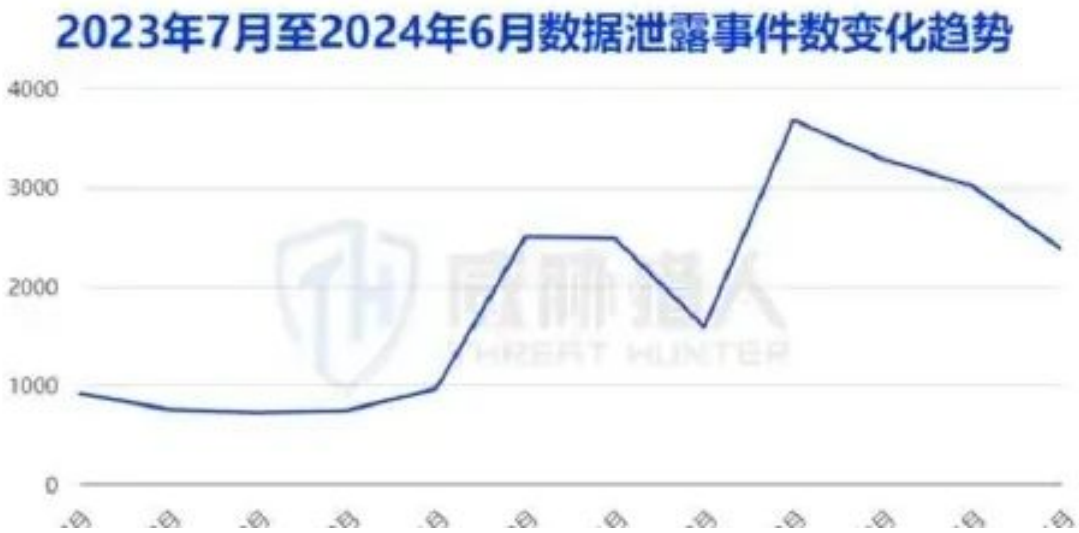
(Feedback from downstream criminal gangs and data sellers must pass iOS, FT, etc.)

Threat Hunter statistics found that in the first half of 2024, there were as many as 1,237 related risk events containing the "iOS" field in the leaked data, an increase of 8 times compared with the second half of 2023.



Data leakage scenario analysis (Chart 1)

Source: Threat Hunter original report, page 58



Data leakage scenario analysis (Chart 2)

Source: Threat Hunter original report, page 58

As the national public security organs intensify their crackdown on traditional phone fraud, operator supervision strengthens, and Facetime becomes more and more popular, criminals begin to focus on the Facetime calling function and try to use this function to commit fraud. The substantial increase in "iOS" data fields and the communication and verification by threat actors

further prove that the current situation of using Facetime for fraud has made the development of the upstream data cleaning industry chain more rampant.

Since 2024, Threat Hunter has discovered that many fraudsters pretend to be "financial platform customer service", "National Credit Center staff" and other identities, use the FaceTime function to initiate calls to Apple mobile phone users, and defraud on the grounds that "millions of dollars in medical insurance need to be closed", "there are outstanding loans that need to be processed", etc., telling mobile phone users that if they do not cancel, they will be forcibly deducted, or their personal credit will be damaged, thereby tricking mobile phone users into transferring relevant funds to designated accounts, causing huge losses to the victims.

(4) In the first half of 2024, there were a total of 657 "file checking" information incidents, and the number of incidents showed a rapid upward trend. It is not uncommon for threat actors to check files through social workers on Telegram and other channels. For example, through a phone number, you can query all the identity information related to the phone number, such as address, bank card number, assets under your name, etc.

File checking: refers to providing investigation or related data extraction services for designated personnel’s information files.

Common file checking services include: trajectory (person trajectory, vehicle trajectory), property in the name (card in the name, car in the name, house in the name), express delivery business (express delivery address, logistics information), personal information (marriage, household registration, social security), etc.

Data leak scenario analysis

Source: Threat Hunter original report, page 59

Among the data breaches discovered in the first half of 2024, Threat Hunter found a total of 657 "archive" information leaks, accounting for 4.10% of the overall data breaches. Judging from the monthly change trend, the number of related risk events related to file checking is on the rise, and the number of related threat actor groups is also increasing. To a certain extent, this reflects that illegal gains through file searches are more common, and the profits behind them are more substantial.

Summary

5. Summary

达 2961 起，成为数据泄露事件数最多的行业。

Data leak scenario analysis

Source: Threat Hunter original report, page 60

In the first half of 2024, the operations of network threat actors will gradually become more intelligent and chain-oriented. Enterprises need to focus on the following issues:

1. In terms of attack resources, in the first half of 2024, except for money laundering bank cards, the cybercrime ecosystem resources showed an increase in magnitude.

Uptrend: The number of risky IPs in the first half of 2024 increased by 44.8% compared with the second half of 2023, and the number of domestic malicious phone numbers increased by 44.8% compared with the second half of 2023.

8. 8%. The number of new bank cards involved in money laundering has declined, down 28% from the second half of 2023.

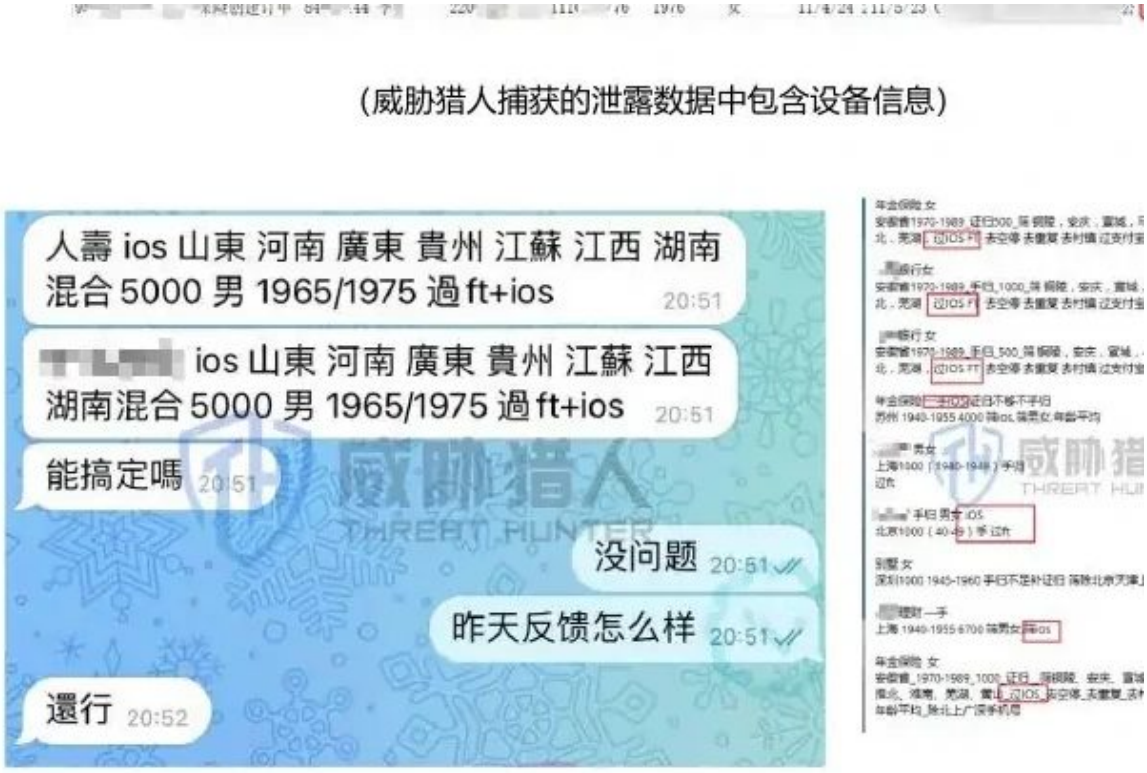
In terms of attack resource application, black card material resource tags are more abundant, such as providing black card category, business information, deactivation time, identification number "filtered", etc., which improves the efficiency of downstream threat actors screening cards and achieves precise malicious activity; in the first half of 2024, threat actors' behavior of maliciously using normal user IPs by implanting Trojans became more rampant. "Hijacking shared agent" IP attacks accounted for more than 67% of the total, becoming the main IP type used by attackers.

2. In terms of attack technology, many threat actors use LSPatch technology to quickly grab orders and conduct malicious activity, based on the automation of HID equipment.

Attacks are more covert. In the first half of 2024, many threat actors used the "LSPatch" technical tool to "quickly grab orders" to conduct malicious activity. Malicious behaviors using LSPatch technology to quickly grab orders were discovered in apps in finance, social networking, real estate and other industries.

In addition, some threat actors have begun to use HID devices to carry out automated operations attacks, through the "HID device + Bluetooth protocol"

"style" to achieve a simple sliding click operation, among which the "short video traffic manipulation" scenario has attracted the focus of cybercriminal groups.



Data leak scenario analysis

Source: Threat Hunter original report, page 62

3. In terms of attack scenarios, threat actors' malicious methods are rapidly updated, and there is a trend of refined division of labor in the malicious activity process.

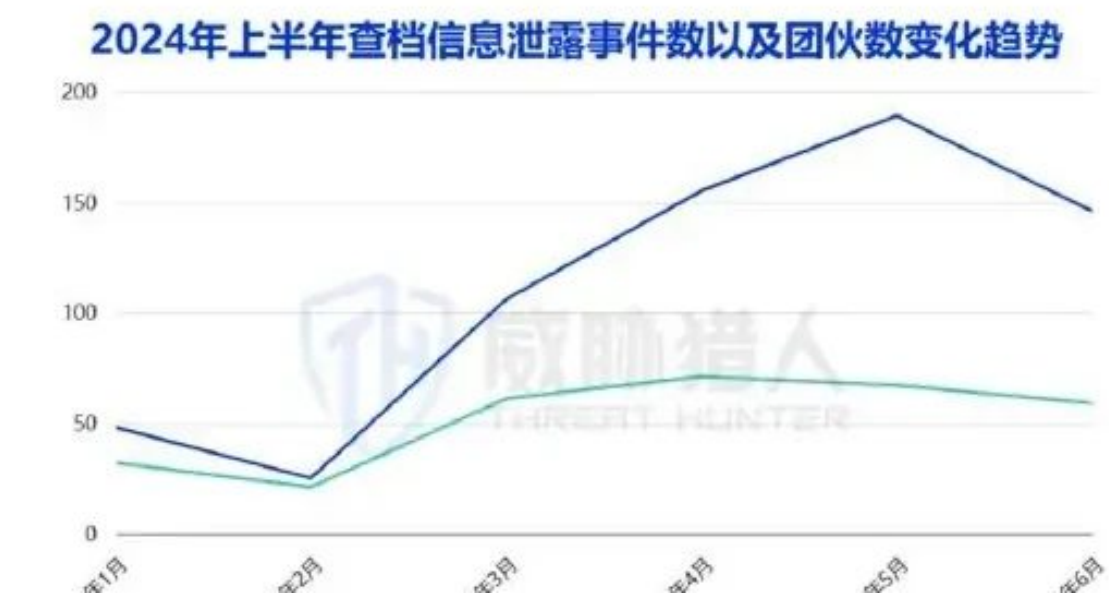
In the marketing fraud scenario, the cybercrime ecosystem group that uses platform rules to make malicious compensation continues to grow. The Threat Hunter intelligence platform has detected a large number of attacks by threat actors known as "super rights defenders." In the first half of 2024, the number of topics related to malicious compensation continued to increase.

In the financial fraud scenario, risk events related to debt fraud occur frequently, and the forgery techniques are more abundant and realistic. threat actors use debtors to conduct one-stop large-amount financing of "housing loans, credit loans, corporate loans, and car loans." The total amount of fraudulent loans by a debtor ranges from 5 to 20 million yuan.

In terms of brand advertising fraud scenarios, Threat Hunter continuously monitors device-based fraud traffic and finds that brand advertising fraud is very common, with the food and beverage category becoming the largest advertiser group suffering from advertising fraud.

In terms of data leakage scenarios, there were many fraud activities using Facetime in the first half of 2024, and the frequency of "device information" field information gradually increased, especially the "iOS" data field. There were a total of 1,237 risk events related to the "iOS" field, an increase of 8 times compared with the second half of 2023.

In response to the endless incidents of evildoing, companies should promptly understand their evildoing processes and details, and establish specific fraud-control rules based on their own business scenarios. The confrontation with external threat actors is dynamic and continuous. Enterprises can rely on cybercrime ecosystem intelligence data based on multi-channel monitoring of the entire network to quickly identify risks and carry out targeted defenses.



Data leak scenario analysis

Source: Threat Hunter original report, page 64