THREAT HUNTER RESEARCH

2023 Annual Cybercrime Ecosystem Research Report

An annual assessment of cybercrime trends, including the growing use of AI, cloud infrastructure and cross-scenario attack resources.

Original publication: 2024-01-29
Research team: Threat Hunter Research Team
Source report: 58 pages

Original report text

This text version is reconstructed based on the 58-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 2023, the number of cybercrime operators exceeded 5.8 million. The number of domestic malicious phone numbers captured by Threat Hunter was as high as 6.25 million, the number of daily active risk IPs was 6.02 million, and the number of money laundering bank cards was 870,000.

Judging from the scale of the million-level cybercrime ecosystem chain and the greatly increased level of attack resources, 2023 will be an unprecedentedly fierce year for the offensive and defensive confrontation between threat actors. The innovative attack resources and technologies have become the "protective color" of threat actors' attacks. Because it is difficult to monitor threat actors' attack behaviors and trace potential risks, many companies have suffered serious losses, which has become a difficult problem that needs to be overcome in business security construction.

Threat Hunter released the "2023 Internet cybercrime ecosystem research annual report", which conducted in-depth research on the cybercrime ecosystem chain in 2023. It conducted a comprehensive analysis from the 2023 Internet cybercrime ecosystem development status, attack resources used by cybercriminal groups, cybercriminal groups attack scenarios and other dimensions. It 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. Money laundering digital wallet: refers to encrypted digital currencies used by threat actors to launder illegal funds, such as consumption through digital renminbi,

Transfer funds by transfer and other methods, and use the concealment of digital currency to evade regulatory review;

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

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

10. Modification: refers to modifying the mobile phone device information, such as mobile phone model, serial number, IMEI, GPS positioning, etc.

The purpose of bypassing company equipment detection;

11. Changing positioning: refers to using relevant tools to modify mobile phone positioning information, such as modifying geographical location information to participate in regional

Activities and conduct marketing fraud;

12. Data leakage intelligence: Threat Hunter captured "unauthorized personal/organizational sensitive information through TG groups, dark web and other channels"

"Information is publicly traded or used", which may include historical data, repeated data, etc., and is often of huge magnitude;

13. 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;

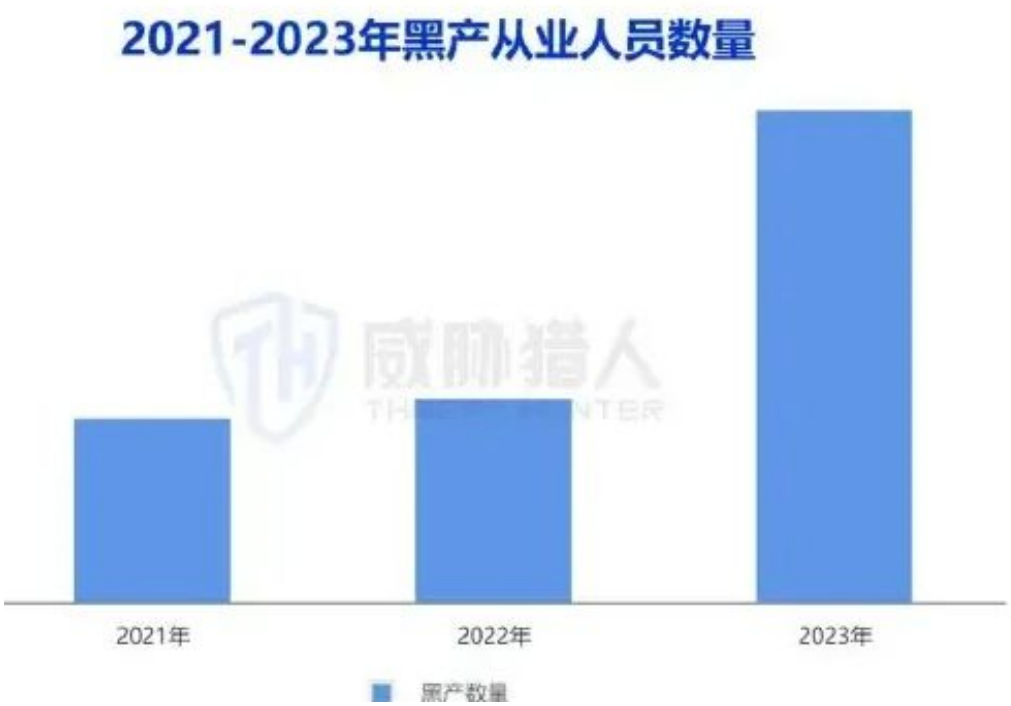
14. Darknet: refers to a hidden network that ordinary netizens cannot search and access through conventional means and need to use some specific software.

software, configuration or authorization to log in;

15. Citizen personal information: refers to citizens' personal identity information, including but not limited to name, ID number, date of birth,

Mobile phone number, home address, bank account information, etc.

Development status of the Internet cybercrime ecosystem in 2023



In 2023, the number of cybercrime-related Internet workers reached 5.87 million, up 141 per cent from 2022.

Source: Threat Hunter original report, page 7

1. Development status of the Internet cybercriminal industry in 2023

1.1 The number of Internet cybercrime operators reached 5.87 million in 2023, an increase of 141% from 2022

Threat Hunter security researchers' survey statistics found that the number of Internet cybercrime operators continued to rise in 2023, with the number of employees reaching 5.871 million, an increase of 141% from 2022.

1.2 Overall situation of the cybercrime ecosystem resources in 2023

1.2.1 Domestic criminal phone numbers increased by 15.44% in 2023 compared with 2022

In 2023, the number of domestic malicious phone numbers reached 6.255 million, an increase of 15.44% from 2022.

1.2.2 The number of risk IPs in 2023 increased by 88.47% compared with 2022

The number of risky IPs will continue to rise in 2023, with the number of risky IPs reaching 6.022 million, an increase of 88.47% from 2022.

1.2.3 The number of money laundering bank cards in 2023 increased by 133.74% compared with 2022

The number of money laundering bank cards will continue to rise in 2023, with the number of money laundering bank cards reaching 874,000, an increase of 133.74% from 2022.

Analysis of attack resources used by threat actors in 2023

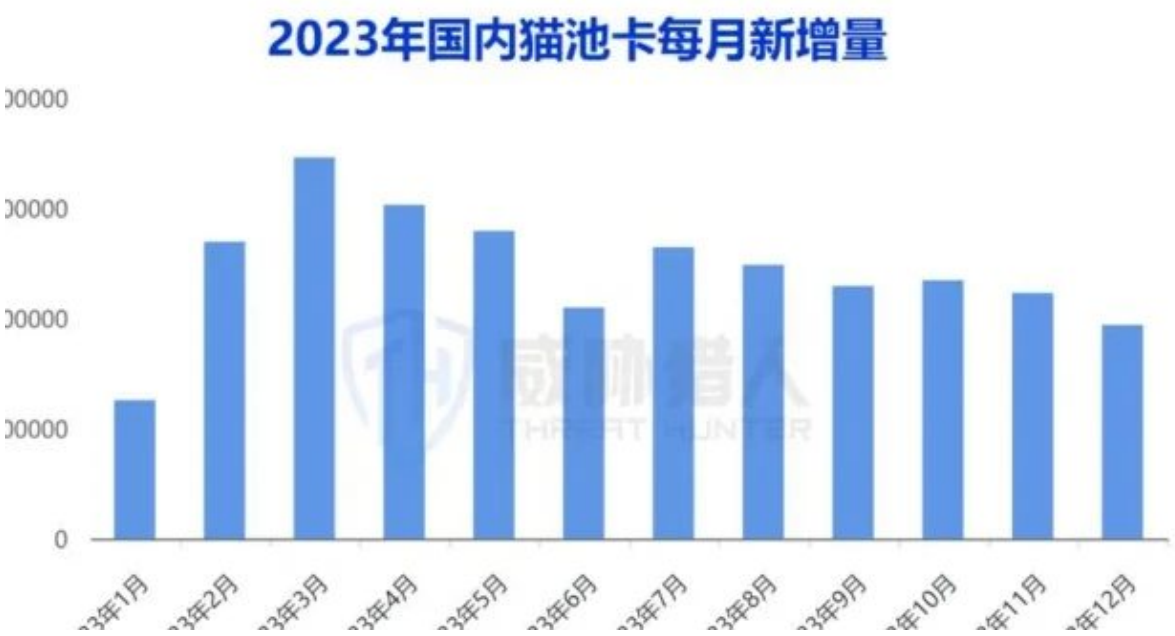
2. Analysis of attack resources used by threat actors in 2023

2.1 Analysis of illicit SIM-card resources in 2023

2.1.1 Change trend of SIM pool cards resources in 2023

(1) The number of domestic SIM pool cards in 2023 increased by 8.25% compared with 2022. According to data from the Threat Hunter threat intelligence operation platform, 5.866 million SIM pool cards will be newly captured in 2023, an increase of 8.25% from 2022. Judging from the changing trend of the number of domestic SIM pool cards in 2023, there was a clear upward trend from January to March and a gradual decrease from April to June.

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



Trends in SIM pool card resources

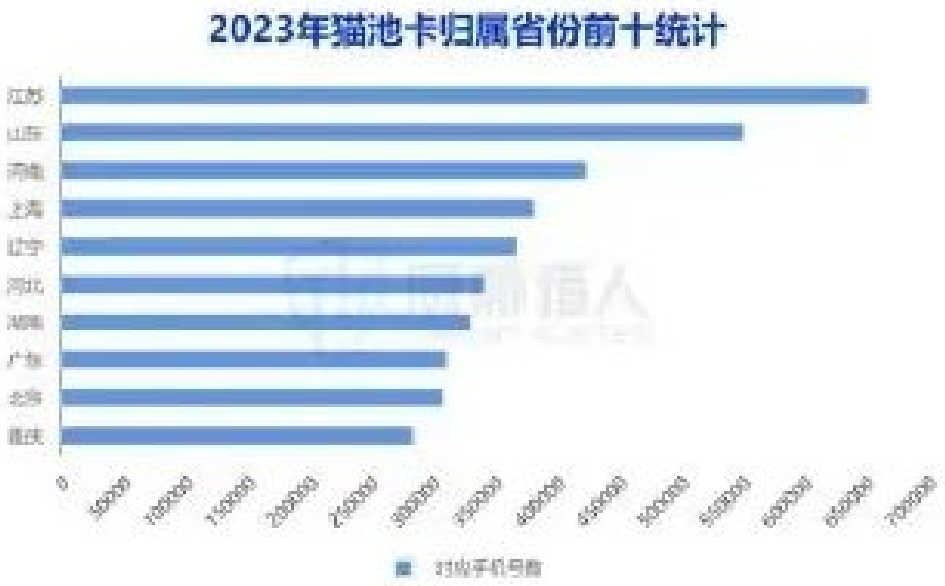
Source: Threat Hunter original report, page 11

From January to March, threat actors connected to a leading SMS verification-code receiving service continued to upload a large number of new verification-code reception phone numbers, causing the number of new malicious phone numbers to continue to rise during this period; from April to June, the leading SMS verification-code receiving service encountered persistent DDos attacks and was unable to operate normally, resulting in a continuous decline in the number of malicious phone numbers during this time period.

(2) The three provinces with the most SIM pool cards in 2023 are: Jiangsu, Shandong, and Henan. Threat Hunter intelligence experts conducted a statistical analysis of the domestic SIM pool cards captured in 2023 and found that Jiangsu, Shandong, and Henan are the three provinces with the most SIM pool cards. Analysis of the cities attributable to them found that Nanjing, Shanghai, and Beijing are the cities with the most SIM pool cards.

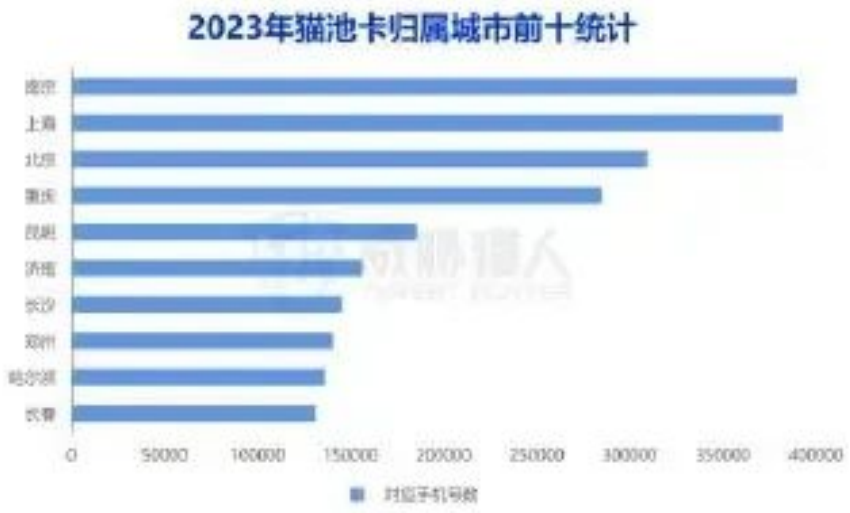
(3) Among the SIM pool cards captured in 2023, 41.78% belonged to the three major domestic operators. In 2023, the Threat Hunter threat intelligence operation platform captured 6.18 million SIM pool cards, of which 41.78% belonged to the three major domestic operators and 58.2% belonged to other operators.

2.1.2 Change trends in interception card resources in 2023



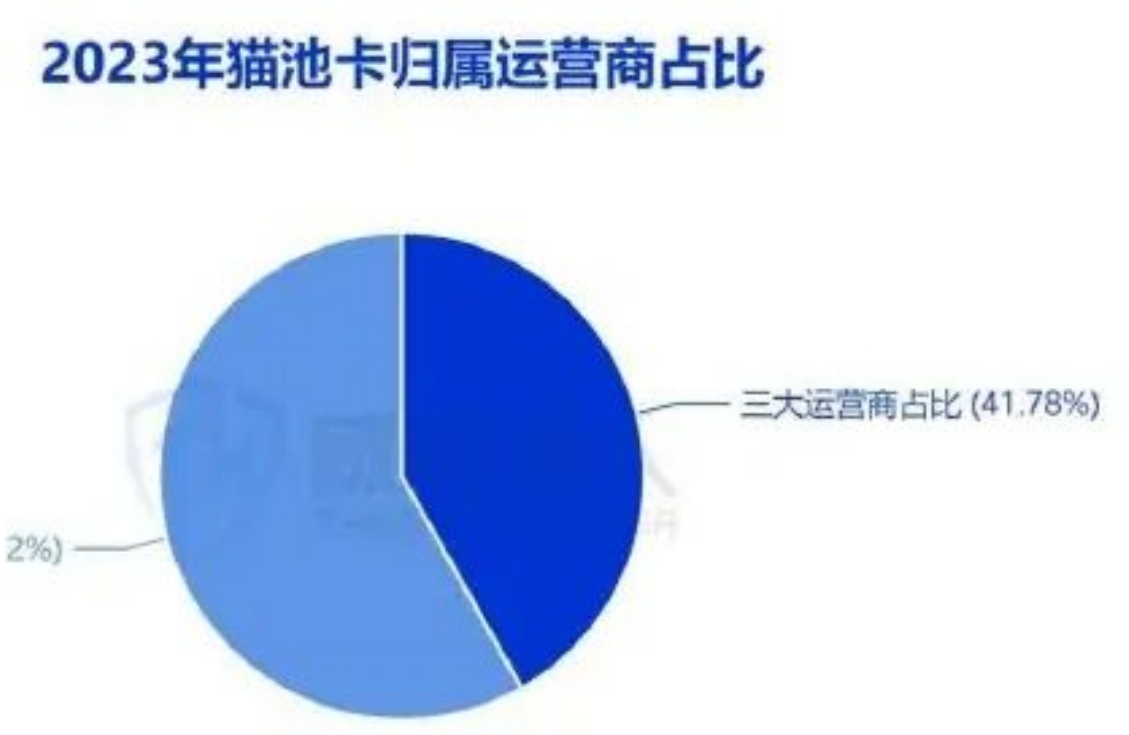
Trends in resource changes in SIM pool cards, 2023 (Chart 1)

Source: Threat Hunter original report, page 12



Trends in SIM pool card resources in 2023 (Chart 2)

Source: Threat Hunter original report, page 12



Trends in SIM pool card resources in 2023 (Chart 3)

Source: Threat Hunter original report, page 12

(1) The number of domestic interception cards reached 389,000 in 2023, with a sharp increase in March. In 2023, Threat Hunter recently captured 389,000 interception cards, and a large number of new interception cards were captured in March. After continuous monitoring and analysis, it was found that the main reason is: the emergence of a new interception card SMS verification-code receiving service in March 2023, resulting in a significant increase in the number of new interception cards in March.

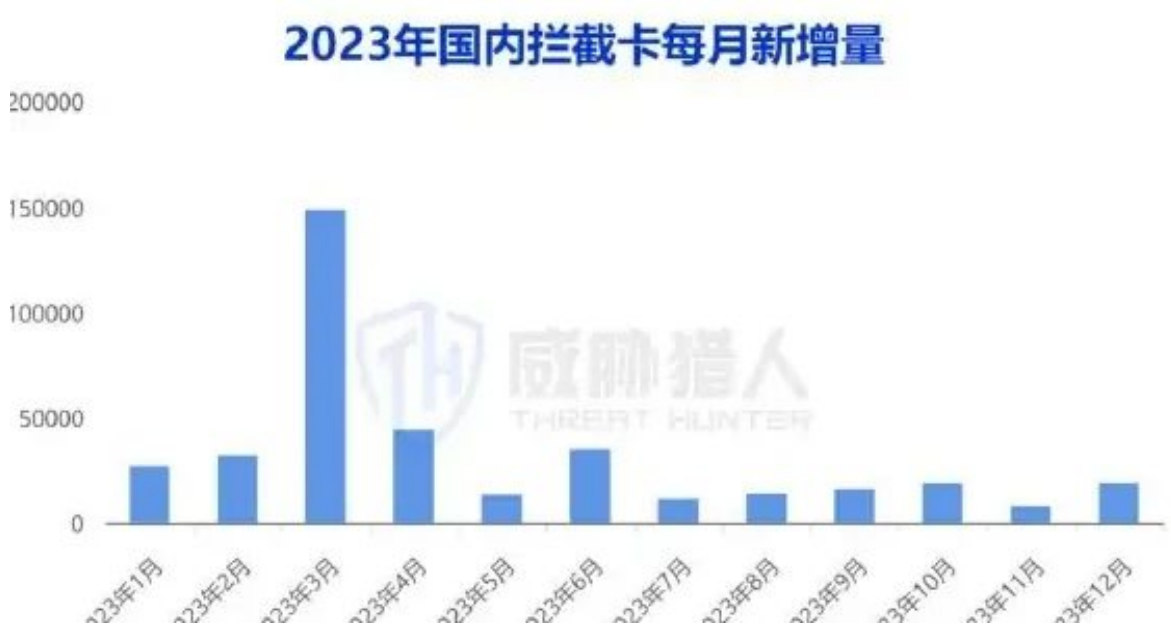
(2) The three provinces with the most interception cards in 2023 are: Guangxi, Shandong, and Jiangsu. Threat Hunter security researchers conducted a statistical analysis of the domestic interception cards captured in 2023 and found that Guangxi, Shandong, and Jiangsu are the three provinces with the most interception cards, and there is a certain overlap with the provinces where SIM pool cards belong. Analysis of the cities attribution found that Nanjing, Guigang, and Nanning are the cities with the most interception cards.

(3) Among the interception cards captured in 2023, 98.48% belonged to the three major domestic operators. In 2023, the Threat Hunter threat intelligence operation platform captured 870,000 interception cards. The interception cards belonging to the three major domestic operators accounted for 98.48%, and the proportion belonging to other operators accounted for 1.52%.

It is worth noting that the number of illicit SIM cards in Segment 192 captured by the threat intelligence operation platform reached 878,000 in 2023, and threat actors used a large number of illicit SIM cards in Segment 192 to conduct malicious activity. Judging from the changing trend of the number of illicit SIM cards in Section 192, there was a significant increase in July, August and October.

According to analysis by Threat Hunter intelligence experts, the main reasons for the large new increases in July, August and October are:

Since the third quarter, 4 supply channels have further increased the investment scale of mobile phone cards in segment 192, further increasing the new increment in the third quarter. In October, some threat actors began to turn their attention to non-head Internet platforms and launch attacks. It was not until November that these platforms began to notice the attacks and conduct fraud controls, and the new increase in segment 192 began to gradually decline.

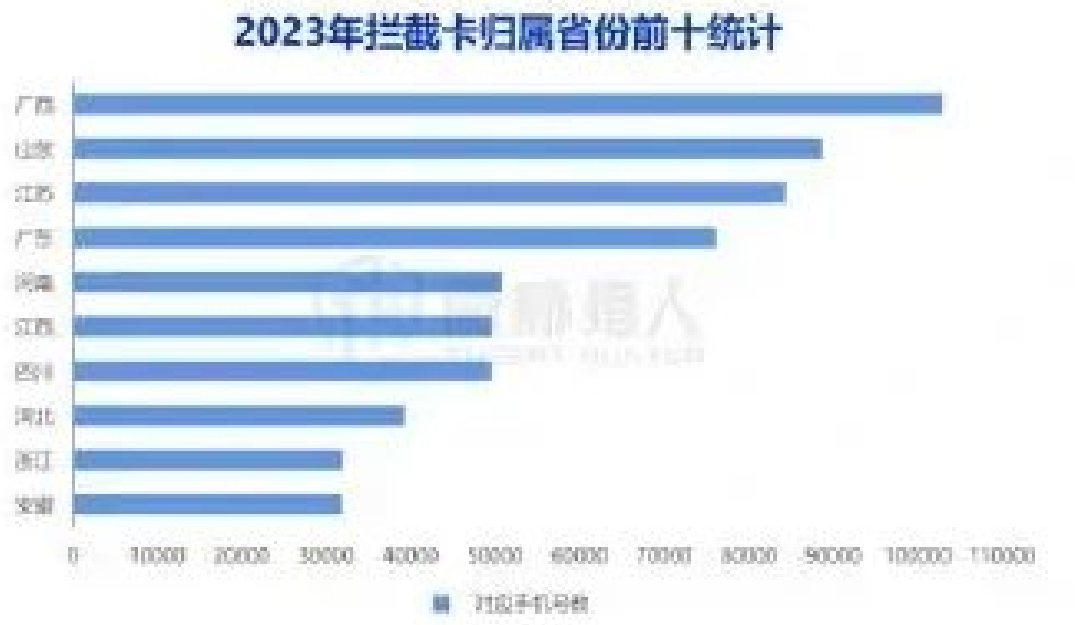


Trends in interception card resources, 2023

Source: Threat Hunter original report, page 13

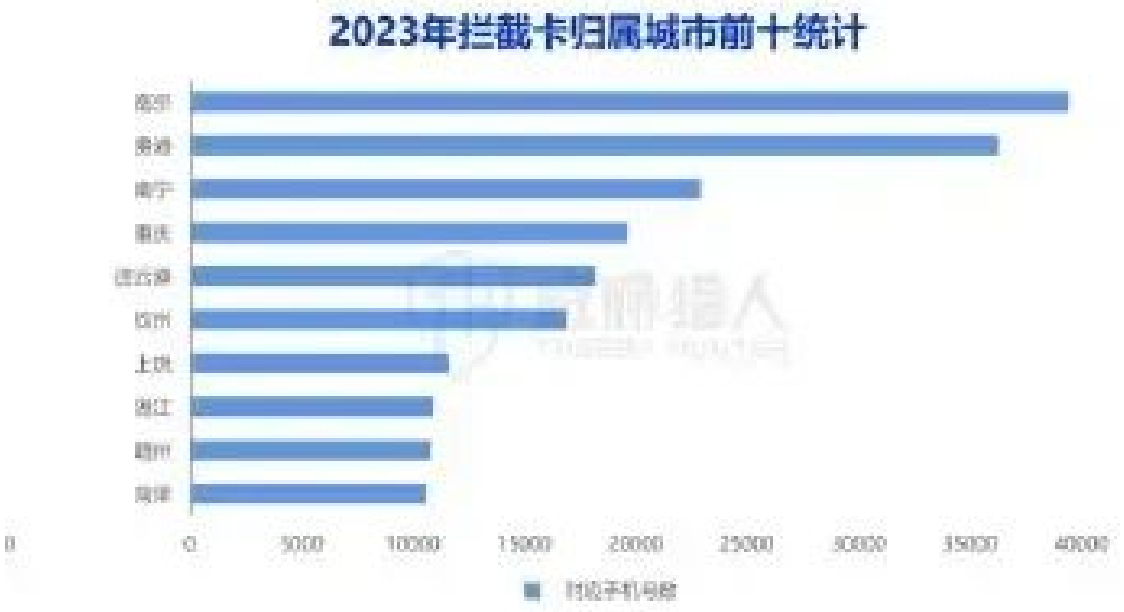
2.1.3 The card issuance platform has become one of the mainstream channels for threat actors to issue high-value code-receiving mobile phone cards.

Judging from the data captured by the Threat Hunter threat intelligence operation platform, the number of card-issuing platforms and card-issuing stores that provide code-receiving services has shown a clear upward trend. At the same time, the number of code-receiving phone numbers captured through the card issuance platform has also shown a clear upward trend. It can be seen that the "card-issuing platform" has become one of the mainstream channels for threat actors to release high-value code-receiving mobile phone cards.



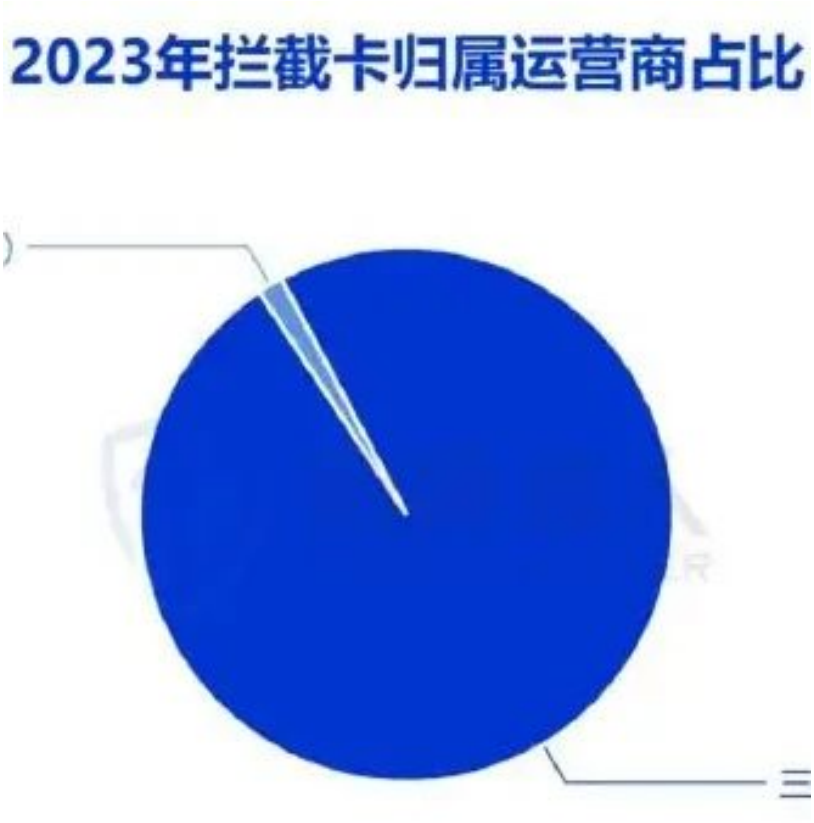
Trends in the flow of intercepted card resources in 2023 (Chart 1)

Source: Threat Hunter original report, page 14



Trends in the flow of intercepted card resources in 2023 (figure 2)

Source: Threat Hunter original report, page 14



Trends in the flow of intercepted card resources in 2023 (Chart 3)

Source: Threat Hunter original report, page 14

High-quality phone numbers that receive codes: The phone numbers have been connected to the Internet for a short time, and the network status is normal. Most of them are physical mobile phone cards newly issued by threat actors card dealers through specific channels and technologies. threat actors mostly use such phone numbers to attack popular app services and make profits, such as the registration and binding services of popular video apps, Internet social apps or e-commerce apps.

(1) The number of card issuance platforms and card issuance stores captured every month in 2023 that involve code acceptance continues to increase. Since January 2023, the number of card issuance platforms that involve code acceptance captured every month continues to rise. As of December 2023, the number of active card issuance platforms has reached 28. Among these card-issuing platforms, the number of card-issuing stores that directly provide phone number receiving services to threat actors has also increased significantly. In December 2023, Threat Hunter captured a total of 322 such stores.

Trends in interception card resources, 2023

Source: Threat Hunter original report, page 15

(2) The number of high-value code-receiving phone numbers captured through card-issuing stores every month in 2023 continues to rise. Since January 2023, Threat Hunter has captured a significant increase in the number of code-receiving phone numbers used for malicious purposes through card-issuing stores.

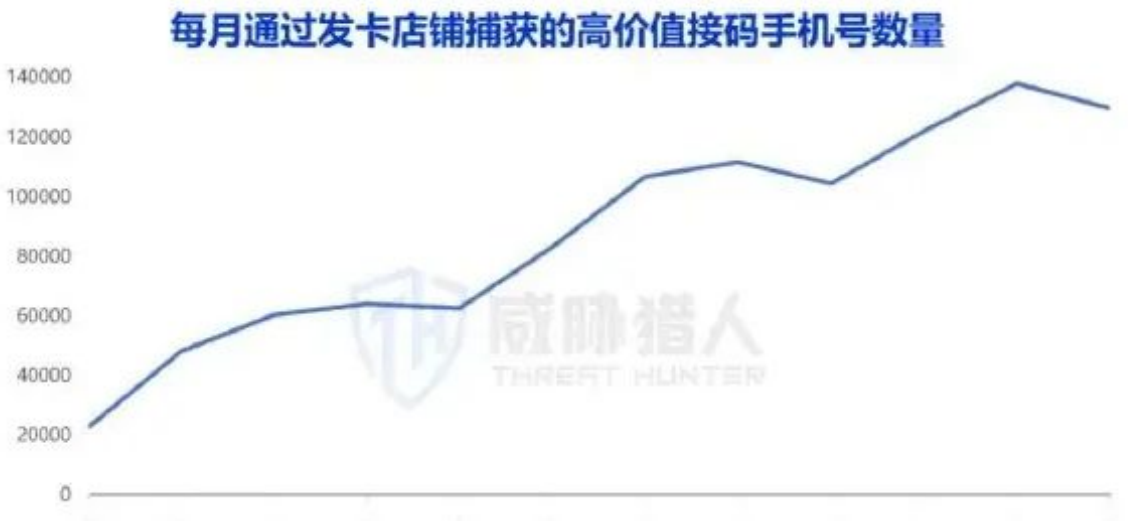
In December 2023, Threat Hunter captured a total of 129,000 malicious phone numbers.

Threat Hunter security researchers discovered: "The cybercrime ecosystem phone number receiving service has become more mature and has shown a clear trend of division of labor."

For example, mobile phone card dealers provide black card materials, and agents bring together multiple card dealer channels to provide covert verification-code reception services for threat actors by opening stores on the card issuance platform.

2.2 Analysis of risk IP resources in 2023

2.2.1 Risk IP resource changes in 2023



The card platform became one of the main channels for cybercrime to deliver high-value handheld cards.

Source: Threat Hunter original report, page 16

In recent years, domestic Internet platform businesses have continued to explore overseas markets. How to identify overseas risky IP has become an issue that major enterprises need to pay urgent attention to. The improvement of Threat Hunter's overseas risk IP monitoring capabilities also provides strong support for Internet platforms to optimize overseas fraud-control rules.

In 2023, Threat Hunter will continue to monitor domestic risk IPs of 59.06 million and foreign risk IPs of 71.72 million. Our analysis of two types of risk IP, domestic and foreign, found:

(1) The three provinces with the most domestic risk IP in 2023: Jiangsu, Zhejiang, and Guangdong

(2) The three cities with the most domestic risk IP ownership in 2023: Shanghai, Chongqing, and Suzhou (3) The three countries with the most foreign risk IP ownership in 2023: Brazil, India, and the United States

(4) Among domestic risk IP types in 2023, home broadband types account for more than 90% (5) Overseas risk IP types in 2023 are mainly home broadband and mobile networks

2.2.2 threat actors’ behavior of maliciously using normal user IPs by implanting Trojans has become more rampant.

Threat Hunter found that threat actors established proxy channels on their networks by implanting Trojans in normal user devices, and each use time was very short, so it was difficult for ordinary users to perceive that their IP had been stolen. From the perspective of customer fraud controls, normal users' IPs are maliciously used by threat actors. This type of IP belongs to "good and bad shared-proxy" IPs.

This type of IP is operated by normal users most of the time, such as clicking, recharging, browsing, etc., but short-term malicious behaviors may occur in a small amount of time. Therefore, the platform may identify the user as a normal user and then ignore his short-term malicious behavior, giving threat actors an opportunity to take advantage.

Through continuous monitoring of the proxy IP platform, we found that threat actors’ malicious use of normal user IPs by implanting Trojans has become more rampant. Take the data captured by Threat Hunter in November and December 2023 as an example: the number of hijacked IPs captured in November reached 5.08 million, and the number of hijacked IPs captured in December reached 9.34 million, an increase of 83.85% from November.

2.3 Analysis of Internet Money Laundering Resources in 2023

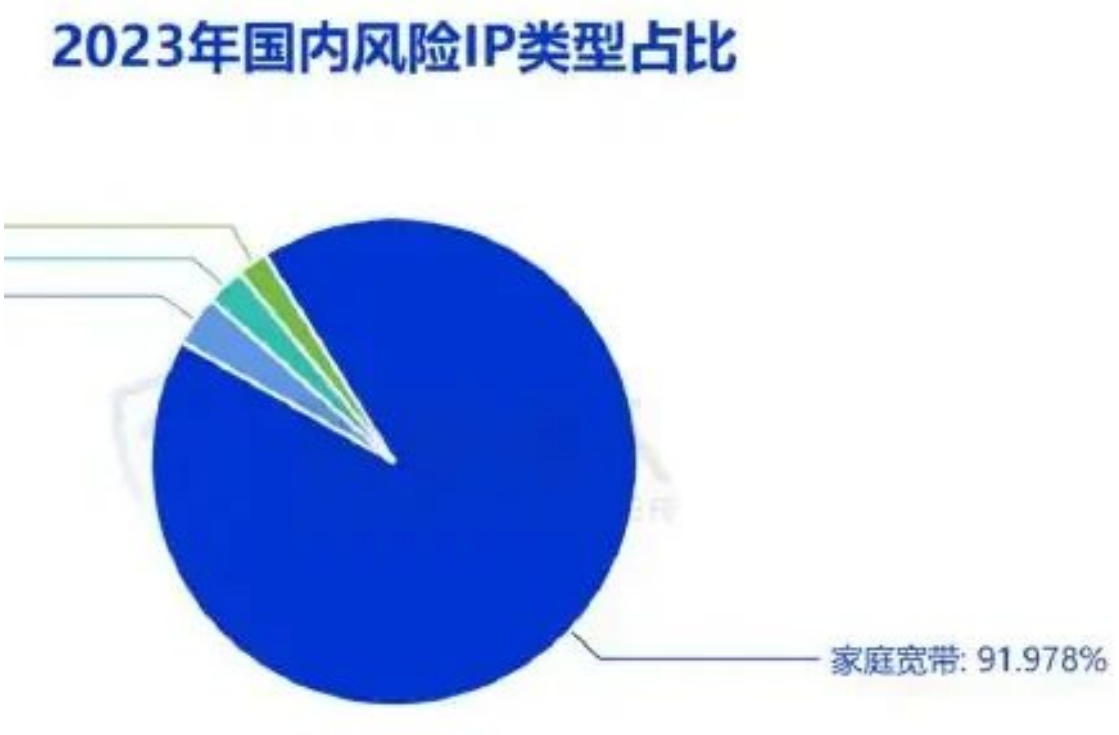
Risk 2023 IP Resource change

Source: Threat Hunter original report, page 17

2.3.1 Changes in bank card resources in 2023

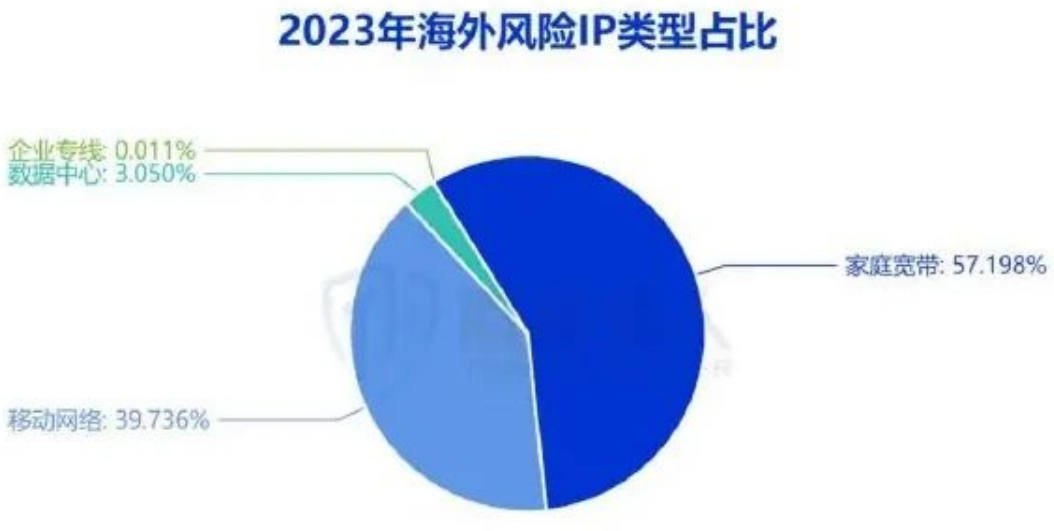
In 2023, Threat Hunter captured a total of 874,000 money laundering bank cards. Further analysis of the captured money laundering bank cards found that:

(1) The proportion of bank cards involved in money laundering belongs to state-owned banks is much higher than that of non-state-owned banks (2) The main range of bank card money laundering amounts is 1,000-5,000 yuan



2023 Risk IP resource changes (Chart 1)

Source: Threat Hunter original report, page 19



2023 Risk IP Resource Change (Chart 2)

Source: Threat Hunter original report, page 19

2023 Risk IP resource changes (Chart 1)

Source: Threat Hunter original report, page 18

2023 Risk IP Resource Change (Chart 2)

Source: Threat Hunter original report, page 18

(3) The time interval between money laundering bank cards is very short, and more than half of the bank cards are used again for less than one day.

2.3.2 Changes in digital RMB resources in 2023

As the public's demand for convenience and security in retail payments increases, digital RMB payment is becoming a new trend in consumption.

Since the "fourth type of digital renminbi wallet" does not need to bind user identity information and can be registered with a phone number, money laundering gangs will use a platform that provides mobile phone accounts and receives verification codes to register digital renminbi wallet accounts in batches, or directly rent or purchase digital renminbi accounts from ordinary people to collect gambling funds.

(1) In 2023, the number of digital RMB wallets involved in money laundering was captured to reach 230,000, with a monthly increase of over 270%. In 2023, Threat Hunter captured a total of 232,000 digital RMB wallets involved in money laundering. At the same time, it was found that threat actors using digital RMB for money laundering were on an overall upward trend, especially in September, with a monthly increase of more than 270%.

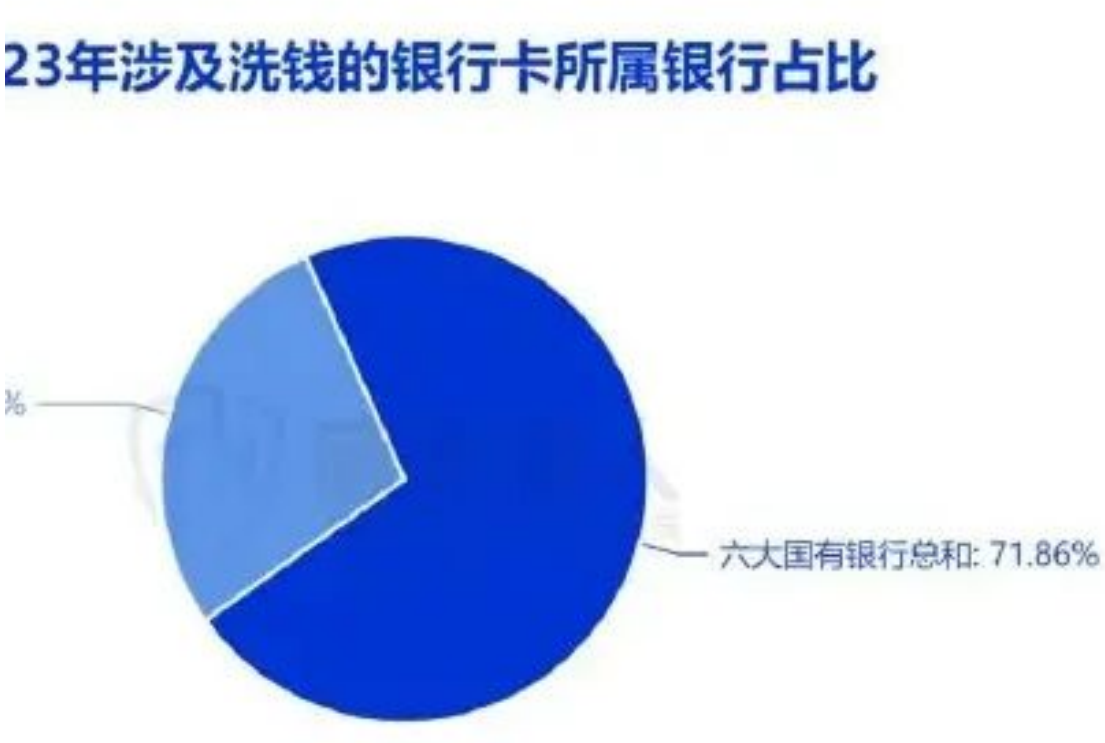
After investigation, it was found that the main reason for the large increase in September was that a large number of fourth-party payment platforms appeared in September that supported digital renminbi money laundering, making the use of digital renminbi for money laundering more frequent.

(2) Over 80% of digital RMB payments involving money laundering are attributed to state-owned banks. Currently, Threat Hunter has monitored that digital RMB money laundering involves dozens of banks, of which state-owned banks account for over 80%. In terms of the number of bank users who support the opening of digital renminbi, the total number of bank users of the six major state-owned banks is much larger than the rest of the banks combined, so their potential digital renminbi users are also relatively large.

2.3.3 Changes in corporate account resources in 2023

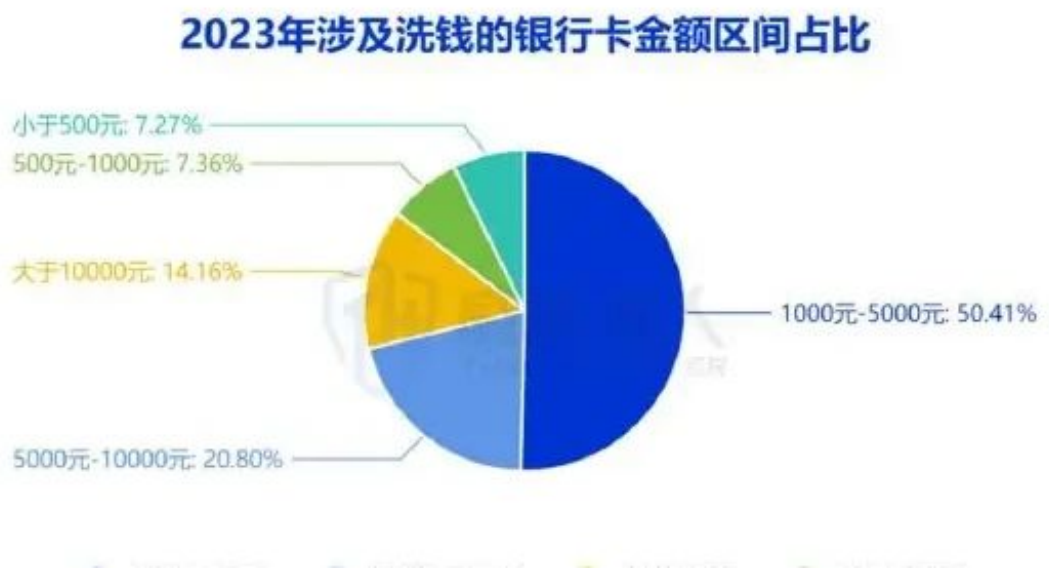
Bank corporate accounts have the characteristics of large collection amounts and high number of transfers. This makes "corporate accounts" often serve as the concentration and divergence points of black money transfers, playing an extremely important position in the money laundering chain of threat actors.

In the process of combating money laundering crimes, it is also very important for banks to conduct fraud controls on public accounts involved in money laundering. Because the collection amount of a public account often ranges from several million to tens of millions, timely discovery of public accounts suspected of money laundering and targeted fraud controls can often interrupt a certain money laundering chain of a certain threat actors group.



Changes in bank card resources in 2023 (Chart 1)

Source: Threat Hunter original report, page 21



Changes in bank card resources in 2023 (Chart 2)

Source: Threat Hunter original report, page 21

In 2023, Threat Hunter continued to cover and 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 increase.

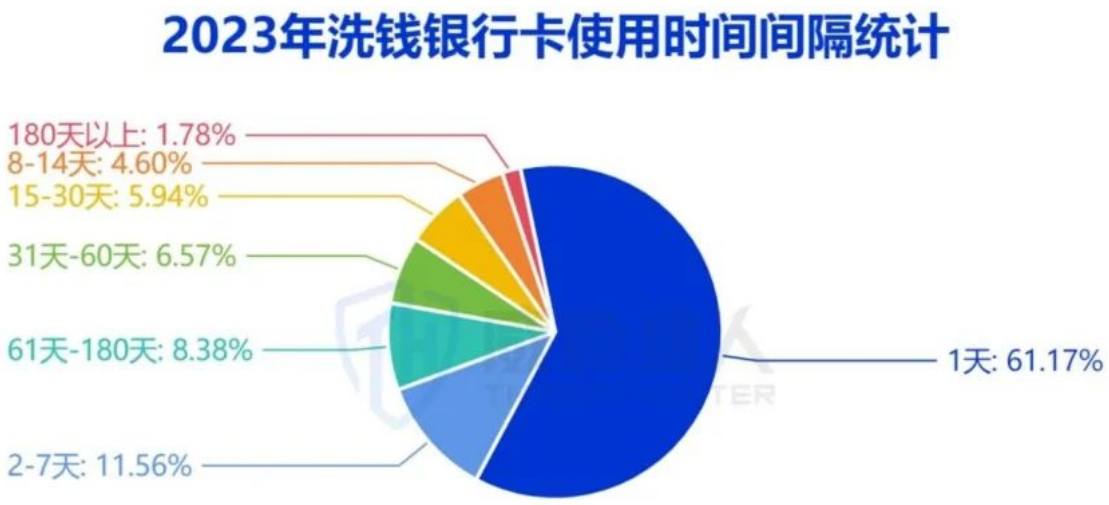
(1) The number of corporate accounts involved in money laundering will be increased month by month in 2023 (2) Among the banks that will capture corporate accounts involved in money laundering in 2023, non-state-owned banks accounted for more than 60%

In 2023, Threat Hunter captured a total of 4,782 corporate accounts involved in money laundering, involving 695 banks. Among the banks affiliated with corporate accounts involved in money laundering, non-state-owned banks accounted for more than 60%.

(3) The three provinces with the most public accounts involved in money laundering were captured in 2023: Guangdong, Shandong, and Henan

(4) The maximum transfer amount used by threat actors for money laundering is 5 million

2.3.4 In 2023, there were as many as 19 money laundering methods used by threat actors, affecting many platforms



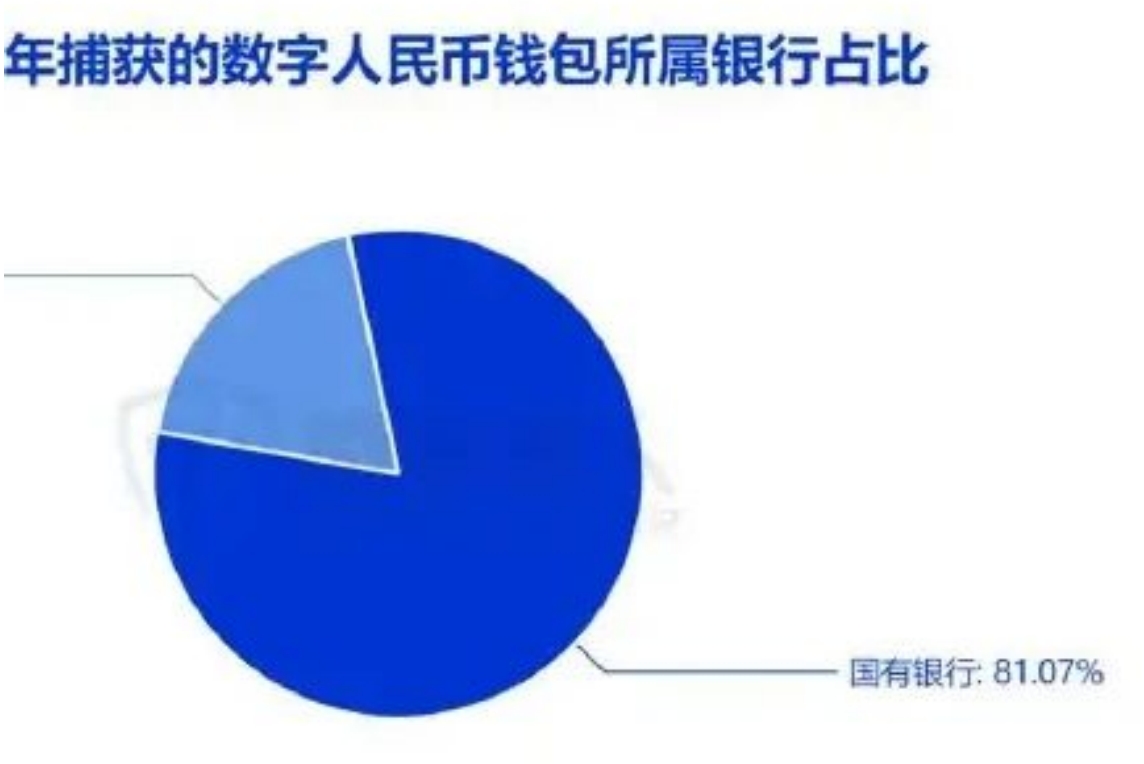
Changes in the digital renminbi money-laundering resources

Source: Threat Hunter original report, page 22

In 2023, Threat Hunter security researchers captured as many as 19 money laundering methods. The malicious methods are constantly iterating and there are many victim platforms.

(1) Introduction to the money laundering process for public accounts 1 What is the public guarantee group?

In order to strengthen the credibility of the channel and ensure the smooth progress of data transactions, both parties to the transaction often use third-party platforms to ensure the credibility and feasibility of the transaction process. The most common method is the "guaranteed public group".



2023 Digital renminbi resource change

Source: Threat Hunter original report, page 23

During the transaction, the buyer and seller will transfer virtual currency equivalent to the transaction amount as a deposit into the virtual currency account provided by the guarantee public group before the transaction; the deposit will be collected through the third-party guarantee public group to avoid losses caused by fraud.

2 How do threat actors use public accounts to launder money through public guarantee groups?

2.4 Risk Email Resource Analysis in 2023

Changes in public account resources in 2023

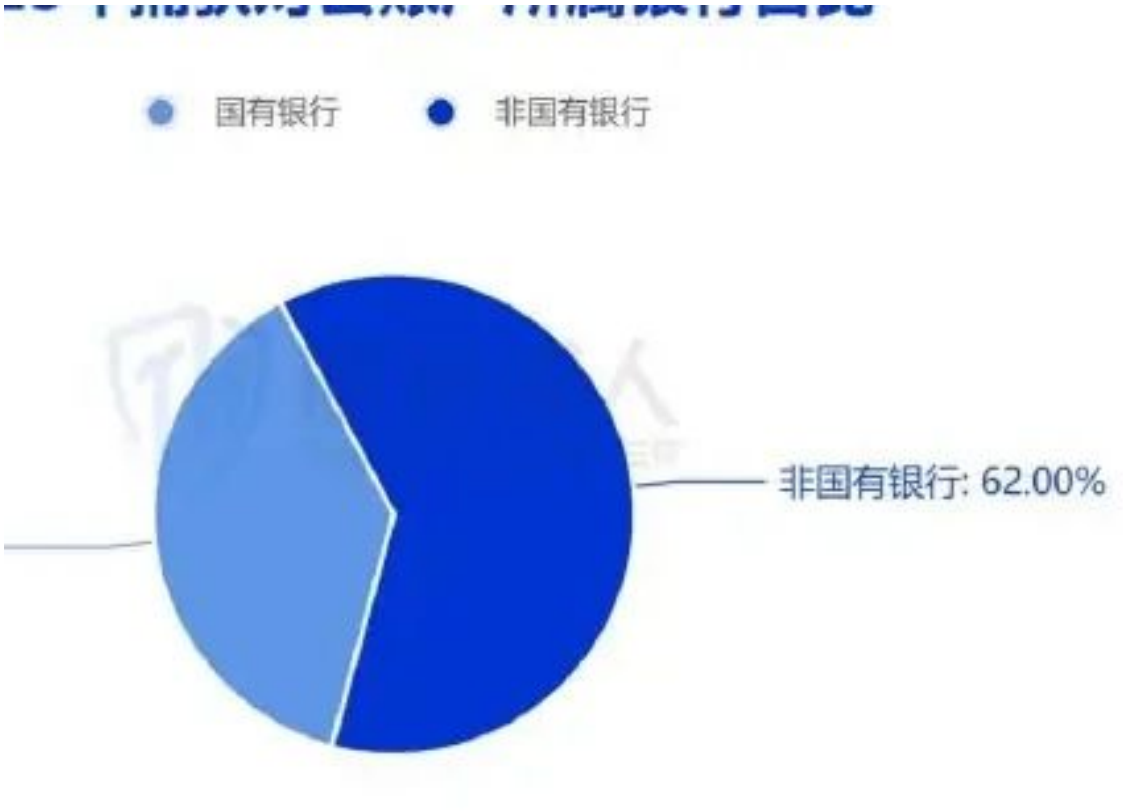
Source: Threat Hunter original report, page 24

2.4.1 Changes in risk mailbox resources in 2023 (1) A large number of risky enterprise mailboxes were captured in September 2023

Judging from the monthly number of different types of risk mailboxes captured in 2023, there was a sharp increase in September. In September 2023, Threat Hunter security researchers conducted MX analysis through known risky mailboxes and associated a large number of risky corporate mailboxes.

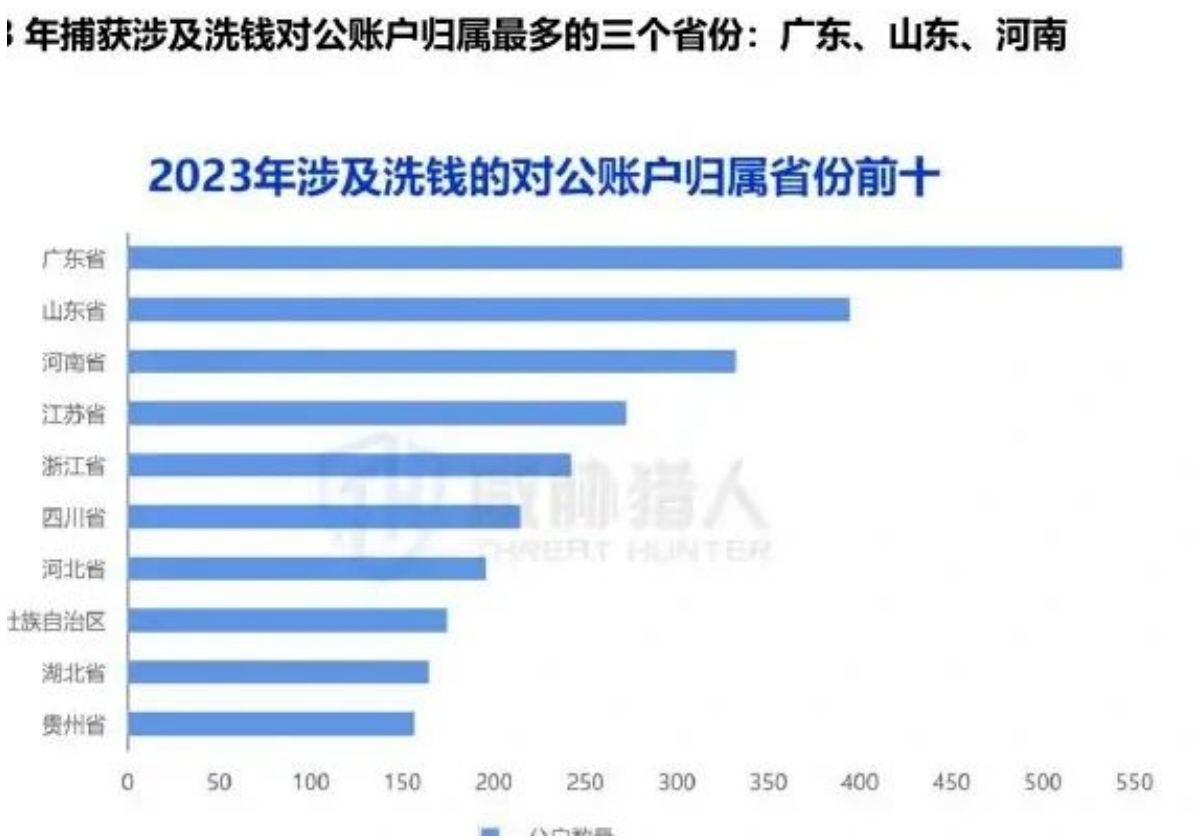
MX, which is Mail Exchanger (Mail Exchange Record), points to a mail server and is mainly used by the email system to locate the mail server based on the address suffix of the recipient when sending mail. Normally, one MX can be bound to multiple email domain names.

(2) Among the risk mailboxes captured in 2023, corporate mailboxes accounted for more than 68%



Changes in public account resources in 2023 (Chart 1)

Source: Threat Hunter original report, page 25



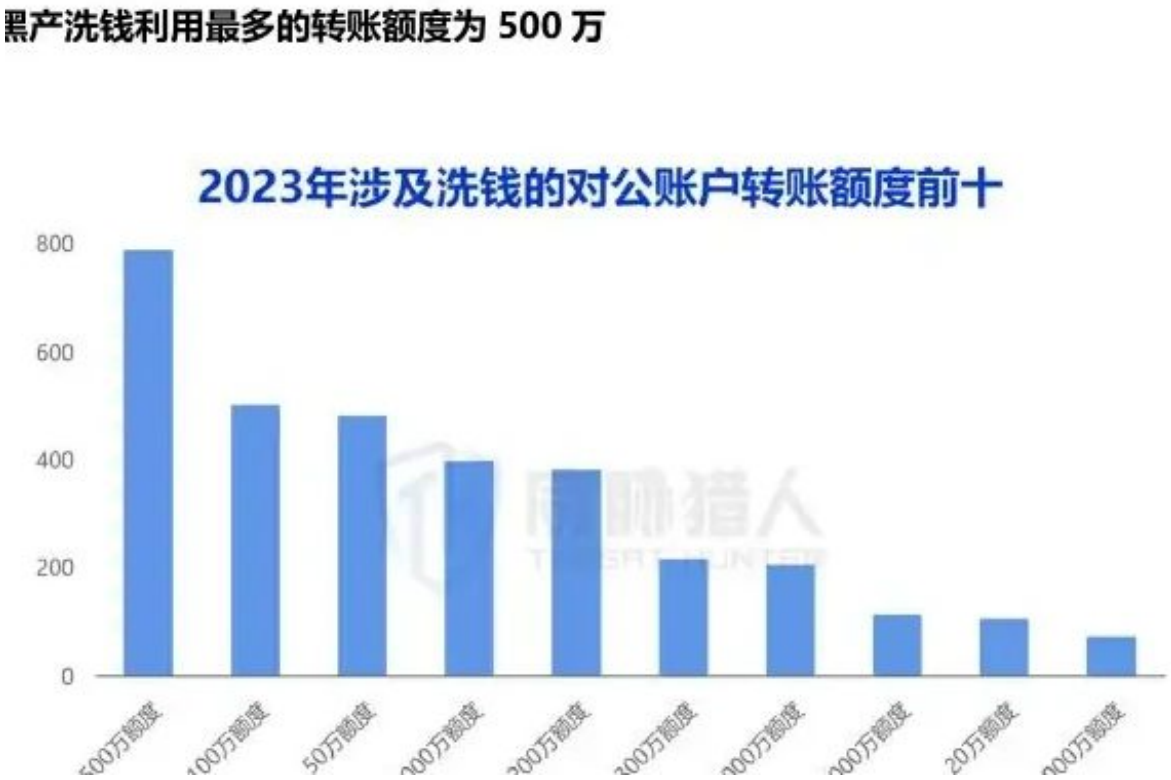
Changes in public account resources in 2023 (Chart 2)

Source: Threat Hunter original report, page 25

Common attack techniques for threat actors in 2023

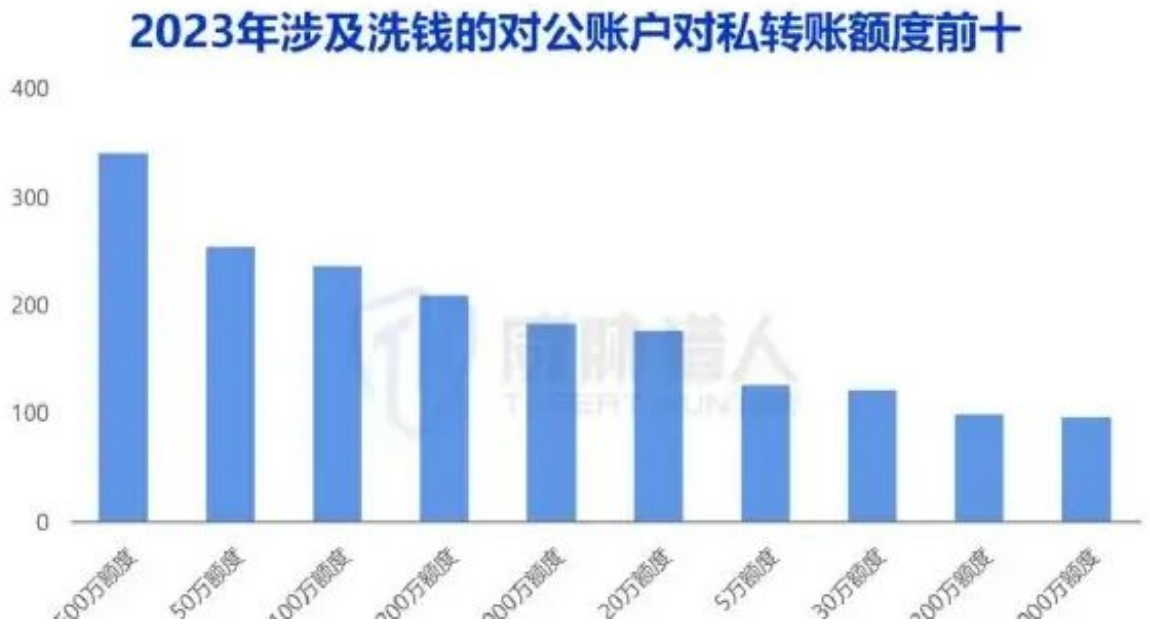
3. Universal attack technology for threat actors in 2023

3.1 threat actors apply AI technology to greatly improve attack efficiency and break through corporate defense systems



As many as 19 methods of money-laundering in 2023, affecting many platforms (Chart 1)

Source: Threat Hunter original report, page 26



As many as 19 methods of money-laundering in 2023, affecting many platforms (Chart 2)

Source: Threat Hunter original report, page 26

In 2023, AI technology will be used in multiple scenarios of network security, and the in-depth application of AI technology has also aroused the covetousness of a large number of threat actor groups. Threat Hunter researchers have observed that many threat actor groups use AI technologies such as text generation, photo activation, face replacement, verification code recognition, and voice generation to attack and commit fraud.

Due to the intelligence and automation capabilities of AI, attackers use AI technology to bypass existing enterprise defenses, launch highly concealed, complex, and automated attacks, and attack as many target users as possible within the same period of time. Therefore, the number of cyberattacks using AI technology has grown rapidly in recent years.

(1) threat actors connect to AI robots in social scenarios to automatically generate chat phrases. Threat Hunter security researchers discovered in the third quarter of 2023 that the cybercrime ecosystem actors have connected to AI robots in social traffic scenarios to make chats more intelligent. Take the captured automatic chat tool "AiTuLing" as an example. In addition to the conventional "draining traffic based on preset words", this tool also supports access to AI robots. At the same time, this tool supports automatic traffic drainage from nearly a hundred social platforms on the market.

Research has found that threat actors purchase the services of AI service platforms and integrate, develop and sell them on this basis, and are ultimately used by more malicious activity gangs to automatically attract traffic and defraud social platforms.

It is worth noting that the access cost of AI robots is also extremely low, as low as 19.9 yuan/month. At the same time, the method of use is extremely simple. You only need to fill in the relevant account number and start the software to automatically chat and drain traffic. It is currently widely used in e-commerce platforms and social group chats, which to a certain extent increases the difficulty of detecting the corresponding platforms.

(2) threat actors use AI to forge videos, and face verification needs to be vigilant

In 2023, threat actors will use AI face-changing tools to produce face-changing videos on a large scale to provide proxy authentication services. Taking social apps as an example, threat actors usually purchase a large number of real-name accounts to attract traffic. When the account triggers platform fraud controls and requires face authentication, AI face-changing technology needs to be used to bypass face verification.

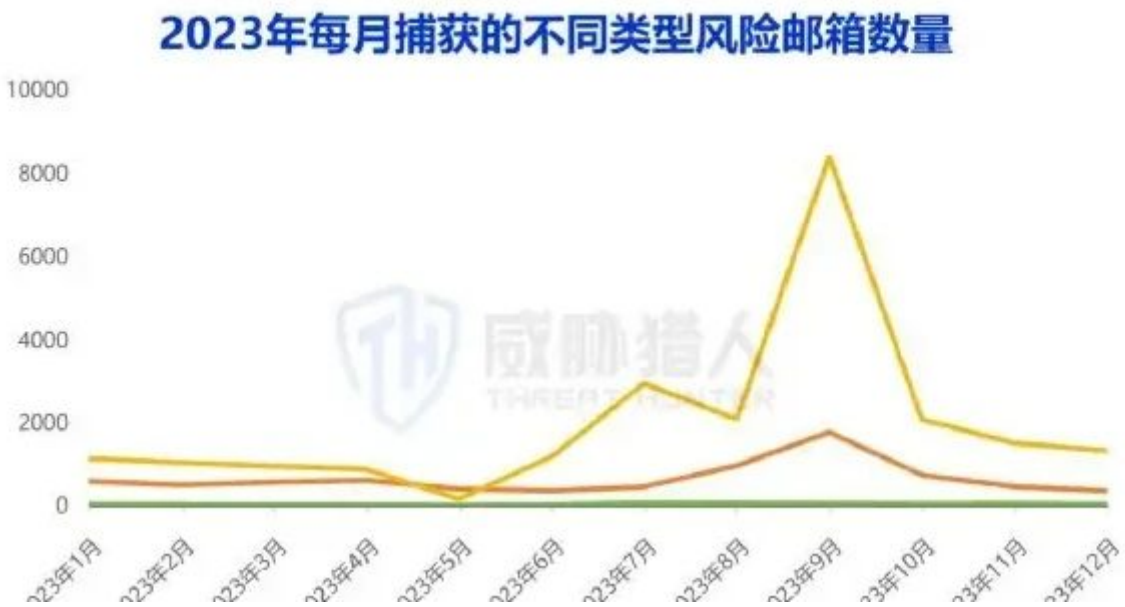
In addition, cases of using conferencing software + AI face-changing tool to pretend to be an acquaintance of the victim to conduct fraudulent transfers occur frequently.

In cases, scammers often ask victims to install conferencing software on their mobile phones, and use the conferencing software + real-time live broadcast face-changing tool to pretend to be a mature person to deceive the victim's trust, and then commit fraud.

Threat Hunter's case of "video conferencing software simulating acquaintances to defraud" is reproduced as follows:

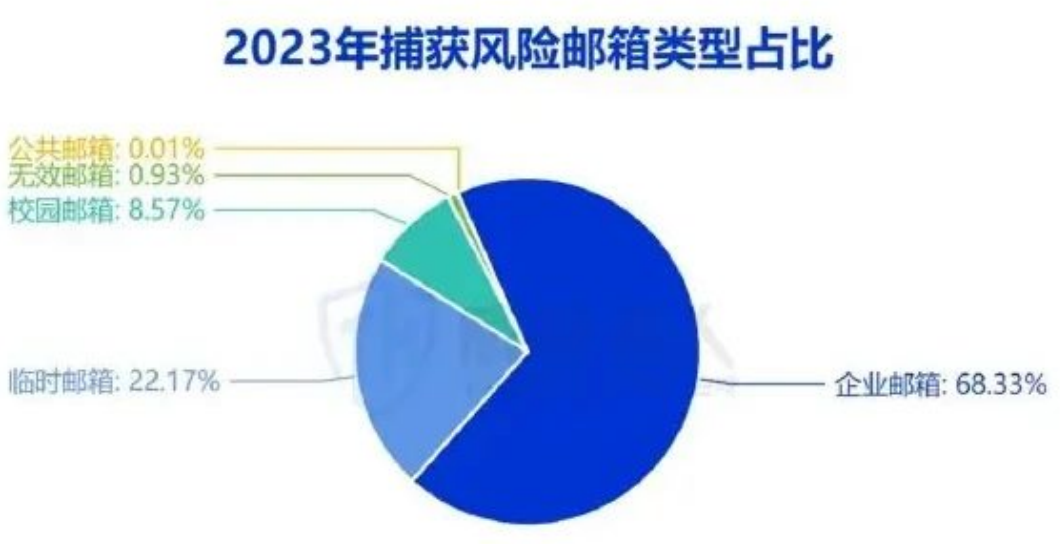
3.2 The number of platforms providing cloud mobile phone services continues to increase, and the supporting attack tools are more complete.

According to research by Threat Hunter, the number of platforms providing cloud mobile phone services will continue to increase in 2023, and leading cloud mobile phone platforms have shown an industrialization trend. In addition to providing cloud mobile phone services, such platforms also provide supporting attack tools, such as proxy IP services, machine modification tools, positioning modification tools, Hook frameworks, etc., which greatly improve the attack efficiency of threat actors. The following table shows the supporting services provided by a certain cloud mobile phone platform:



Risk mailbox resource changes in 2023 (1) Large number of venture mailboxes captured in September 2023 (Chart 1)

Source: Threat Hunter original report, page 30



Changes in risk mailbox resources in 2023 (1) Large number of venture mailboxes captured in September 2023 (Chart 2)

Source: Threat Hunter original report, page 30

Compared with real mobile phone devices, cloud phones have the following advantages:

(1) Low purchase cost: purchasing a real mobile phone costs hundreds to thousands of yuan, while renting a cloud mobile phone only costs tens of yuan/month;

(2) Easy to use and complete supporting services: Cloud mobile phones come with built-in modification tools and supporting services such as virtual positioning and automated script tools.

The advantages of the above cloud mobile phones greatly reduce the cost of threat actors' attacks. At the same time, they save the time required for threat actors to install and configure the malicious activity environment, improve the attack efficiency of threat actors, and bring certain challenges to corporate fraud controls.

In addition to Android cloud phones, it is not uncommon for threat actors to use iOS cloud phones to conduct malicious activity. Due to the strict restrictions of the iOS system on application permission applications, it is much more difficult for most Internet companies to obtain device information on iOS devices than on Android devices. This may make it more difficult for the platform to conduct fraud-risk detection on iOS devices to a certain extent.

In response to such situations, Threat Hunter recommends that companies should obtain samples of such platforms in a timely manner and conduct relevant sample analysis and defense.

Analysis of threat actors attack scenarios in 2023

4. Analysis of threat actors attack scenarios in 2023

4.1 Analysis of business fraud scenarios in 2023

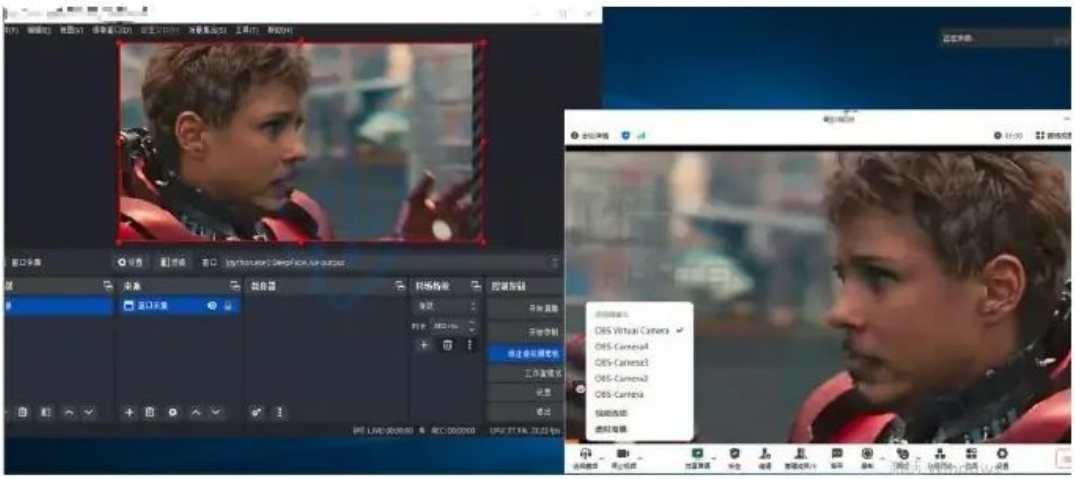
4.1.1 Marketing activities

IA technology has significantly increased the efficiency of attacks and breached the corporate defense system.

Source: Threat Hunter original report, page 33

(1) 9.28 million pieces of marketing activity attack intelligence, involving 159,000 malicious threat actors. This year, the current situation of marketing activities on various corporate platforms being attacked by threat actors remains severe. In 2023, Threat Hunter captured a total of 9.28 million marketing activity attack intelligence pieces, and detected 12,000 active malicious social groups, involving 159,000 malicious threat actors.

威胁猎人对“视频会议软件模拟熟人进行诈骗”的案例复现如下：



IA technology has significantly increased the efficiency of attacks and breached the corporate defense system.

Source: Threat Hunter original report, page 34

(2) A large number of threat actors used loopholes in business rules to obtain user discounts. In December 2023, Threat Hunter discovered that a large number of cybercrime-related and promotion-abuse actors used the method of "refunding through official channels after purchasing through third-party channels" to obtain immediate discounts from banks and platforms. This resulted in a large number of abnormal refund orders on the cooperative platform, and at the same time, the instant discounts for activities were also stolen in vain. Mainly because threat actors take advantage of the fact that there is no information exchange between the third-party platform that provides purchasing services and the official platform.

(3) The crowdsourcing platform is “private” and malicious activity behaviors are more hidden. In 2023, Threat Hunter researchers discovered that cybercriminal groups have launched a more complex and secure crowdsourcing release channel in order to avoid monitoring and fraud controls of the crowdsourcing platform. Its complexity is mainly reflected in:

1. First of all, crowdsourcing personnel need to enter a specific social group chat to obtain the website link of the crowdsourcing platform;

2. Crowdsourcing personnel then need to access the link and register and log in before they can perform the order-taking task.

Although placing orders in this way increases execution time and operating costs, its concealment makes the monitoring and fraud controls of the platform much more difficult.

In addition to private crowdsourcing platforms, Threat Hunter has also observed that some public crowdsourcing platforms have also begun to introduce new strategies to prevent the platform from being monitored and restricted, such as:

1. In the volume traffic manipulation task, the traffic manipulation link uses a short link instead of the real volume traffic manipulation link;

2. In the new task, you need to register, use the real-name crowdsourcing app, and receive the task to obtain detailed task steps and tutorials.

(4) The current situation of e-commerce sales is severe, and daily chemical fast-moving consumer goods and beauty cosmetics and skin care products have become the hardest-hit areas for e-commerce sales. In 2023, among the offline sales plans captured by Threat Hunter, the top three offline sales categories are daily chemical fast-moving consumer goods, beauty cosmetics and skin care, and medical equipment, accounting for 55.35%, 20.09%, and 8% of the total respectively. The remaining 16.56% of the categories are related to health products, home appliances, mobile digital phones, fashion clothing, alcohol, etc.

4.1.2 Credit fraud

(1) There are 1.96 million pieces of credit fraud attack intelligence, and 4,486 active groups were monitored. In 2023, Threat Hunter captured a total of 1.96 million pieces of credit fraud attack intelligence, monitored 4,486 active malicious activity social groups, and 28,000 malicious activity threat actors; although the number of active malicious activity groups and the number of malicious activity threat actors changed relatively steadily in 2023, the platform still needs to be alert to the credit fraud cybercrime ecosystem.

(2) Anti-collection techniques and cases Anti-collection usually refers to the behavior of some organizations or individuals to help debtors maliciously avoid debts through abnormal means, help debtors extend the repayment period, reduce interest charges, or reduce the debtor's repayment liability through other means.

For example, the anti-collection agency asks the debtor to send a personal phone card or set up a call transfer, and the so-called legal personnel of the anti-collection group negotiate and communicate on behalf of the debtor to achieve goals such as interest reduction and exemption and deferment/installment repayment. Finally, based on the anti-collection results, a certain percentage of handling fees will be charged to the debtor, thereby making a profit.

After investigation, it was found that there are four main roles in anti-collection malicious activity scenarios:

针对此类情况，威胁猎人建议企业应及时获取此类平台样本，进行相关样本分析和防御。

The number of platforms providing cloud cell phone services continued to increase, with better tools to support attacks

Source: Threat Hunter original report, page 36

1 Lender: Feed back the demand for interest extension and suspension, and seek help from an anti-collection agency;

2 Anti-collection agency: Publish anti-collection business advertisements on various social platforms/channels to solicit overdue loan borrowers 3 Legal affairs: Apply to the online lending platform for negotiation extension and negotiate on behalf of the borrower 4 Lending platform: Agree to negotiate an extension under the threat of legal rhetoric

The following is the operational process of deferred interest suspension for overdue loans:

4.1.3 Content flushing

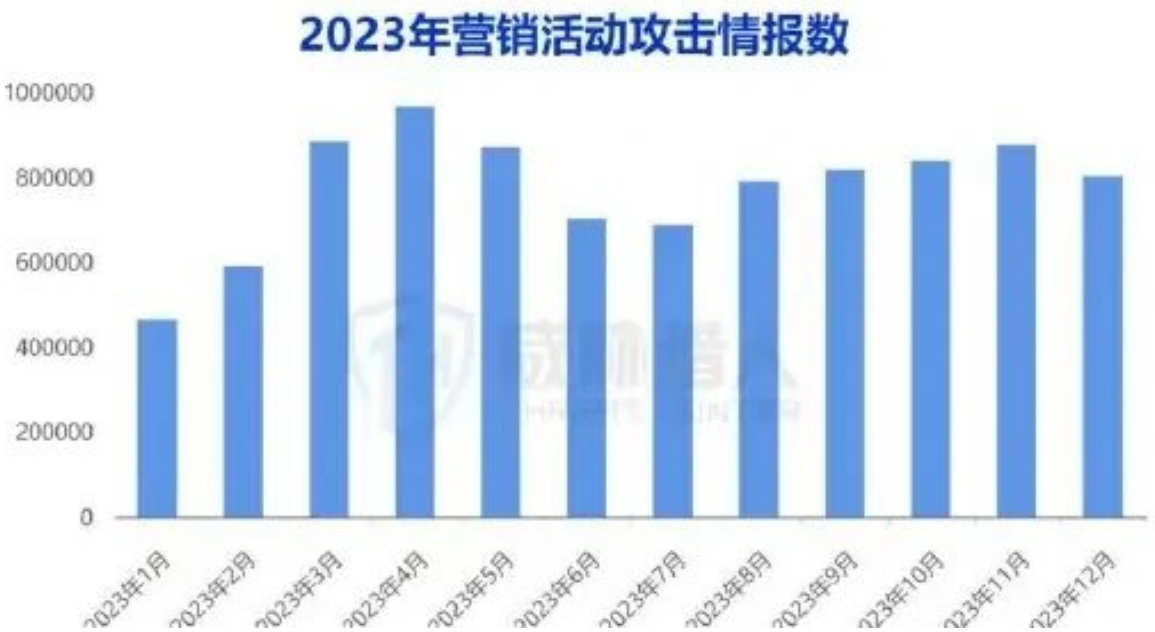
In 2023, the overall traffic manipulation and fraud situation remains severe. Threat Hunter captured a total of 425,000 traffic manipulation and fraud attack reports on live broadcast platforms, content platforms, e-commerce platforms and application download platforms, monitored 4,364 active traffic manipulation malicious activity social groups, and the number of malicious threat actors reached 5,759.

In terms of traffic manipulation methods, as major platforms have improved their ability to identify malicious traffic manipulation behaviors, many traffic manipulation studios have gradually reduced protocol traffic manipulation and group control traffic manipulation based on real devices, and switched to human-operated traffic manipulation.

(1) Live broadcast platforms and content platforms are the most severely affected by traffic manipulation attacks

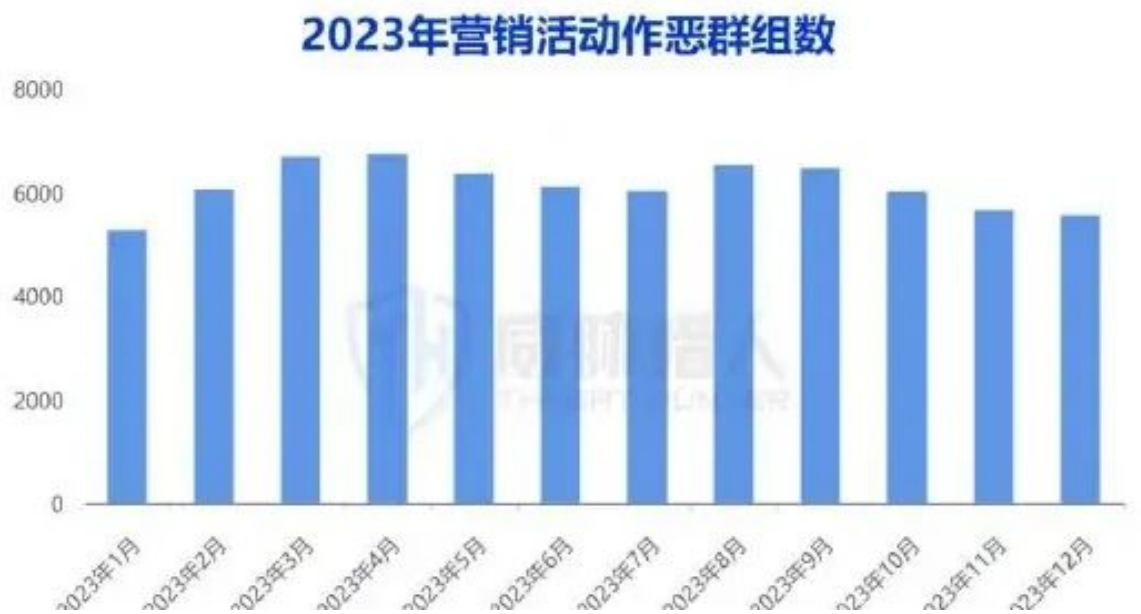
(2) human-operated fraud and traffic manipulation are still the mainstream method of traffic manipulation (3) The after-sales service of traffic manipulation is improved, and threat actors provide "replenishment" services. As the ability of major platforms to identify malicious traffic manipulation behaviors improves, the amount of traffic manipulation in the same batch often fails to reach the established target number. At this time, threat actors usually perform supplementary operations, that is, "within a specified period of time, through continuous traffic manipulation, the number of views and clicks of the article or video can be maintained at the established target number."

.8 万条，监测到活跃的作恶社交群组 1.2 万个，涉及作恶黑产人数达 15.9



Marketing activities (Chart 1)

Source: Threat Hunter original report, page 38

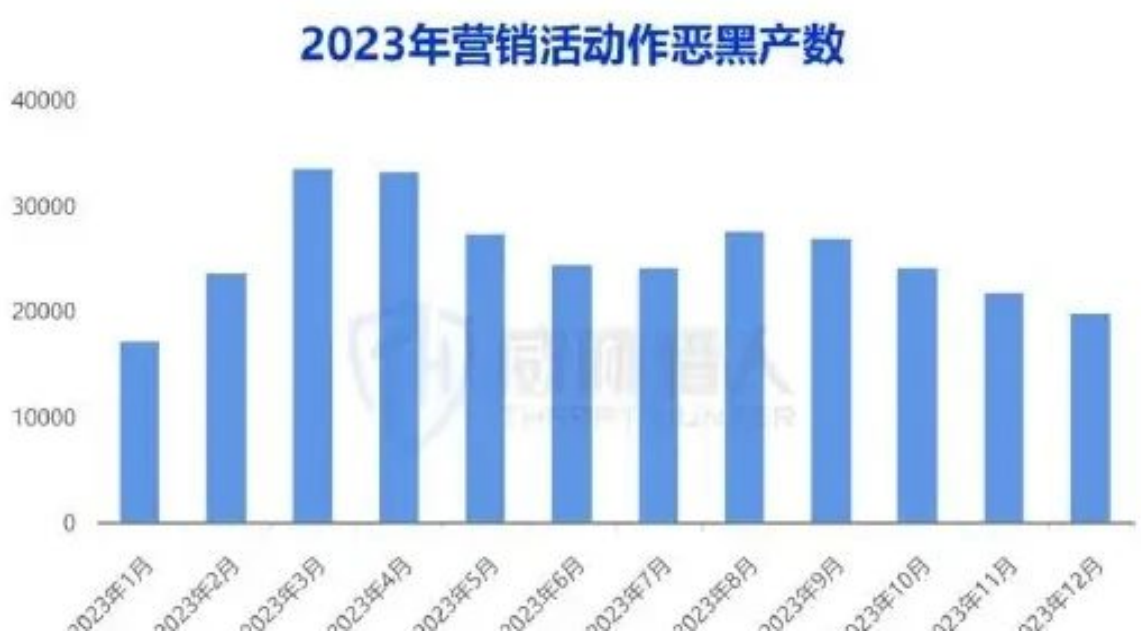


Marketing activities (Chart 2)

Source: Threat Hunter original report, page 38

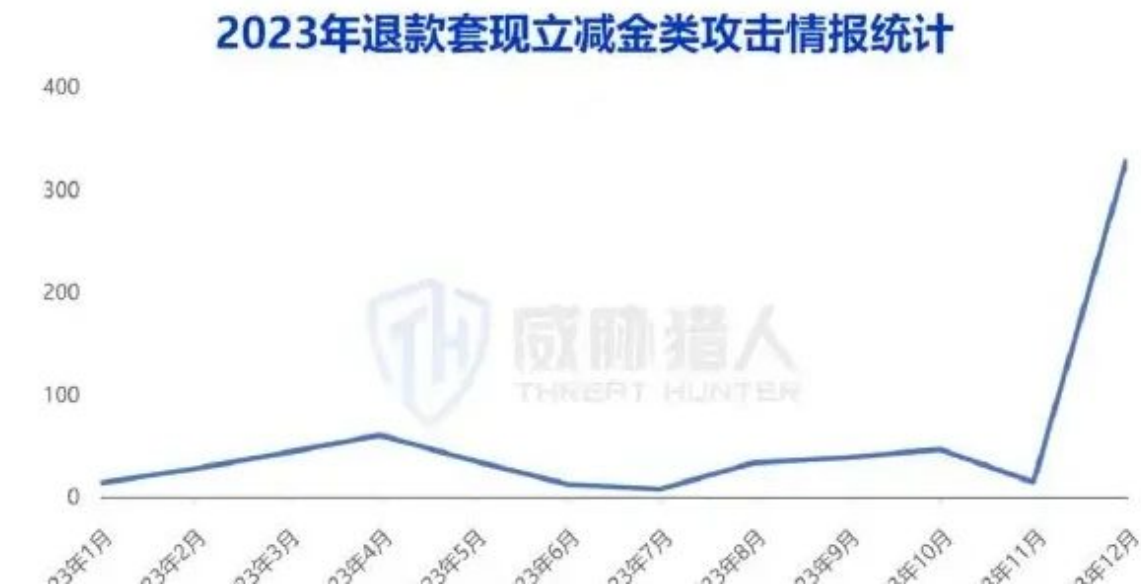
4.2 Analysis of data breach scenarios in 2023

(1) More than 19,500 data leakage incidents will be monitored in 2023, and industries such as finance, logistics, and aviation are the hardest hit by data leakage. According to data from the Threat Hunter data leakage risk monitoring platform, among the nearly 150 million pieces of intelligence monitored across the entire network in 2023, there were more than 19,500 valid data leakage incidents that have been analyzed and verified. From the perspective of industry distribution, data breaches in 2023 involve more than 20 industries, and the top five industries with the number of data breaches are finance, logistics, aviation and travel, e-commerce, and automobiles.



Marketing activities (Chart 1)

Source: Threat Hunter original report, page 39



Marketing activities (Chart 2)

Source: Threat Hunter original report, page 39

(2) The financial industry ranked first with 8,758 data breaches, and the aviation industry jumped to third place. In 2023, the financial industry is still the hardest hit area for personal information leaks, with 8,758 data breaches involving information of high-net-worth individuals in banking, insurance, securities and other industries, mainly due to the higher value of profits used by downstream threat actors for marketing promotion and fraud.

From the perspective of financial sub-sectors, the banking industry has the largest number of data breaches, with a total of 4,293 incidents occurring throughout the year, followed by the online lending, insurance, securities and payment industries.

(3) "Citizen personal information" will still be the main type of data leakage in 2023, accounting for more than 90%. From the perspective of data leakage types, there are three main types of data leakage in 2023: 18,347 cases of citizen personal information (93.68%), 727 cases of sensitive code (3.71%), and 510 cases of sensitive documents (2.6%).

(4) More than 50% of citizens' personal information is traded at night, and more than 30% is traded on non-working days. Threat Hunter research statistics found that among the data transaction times in citizen personal information leakage incidents in 2023, the number of incidents that occurred on non-working days (weekends and holidays) was as high as 31.21%, and the proportion of incidents that occurred at night was as high as 51.88%, more than half.

(Night: 18:30 to 09:30 the next day)

When the defense is at its weakest, it is difficult for enterprises to quickly sense and respond in a timely manner when a data breach occurs, so that they miss the best response opportunity, which has a significant impact on corporate funds, brand reputation and business competition.

Marketing activities

Source: Threat Hunter original report, page 41

(5) Reasons for data leakage include operator channel leakage, insider leakage, hacker attacks, etc. From the specific causes of data leakage, the causes of data leakage in 2023 include operator channel leakage, insider leakage, hacker attacks, security awareness issues, etc. Among them, the number of data leakage incidents caused by operator channel leakage is the largest.

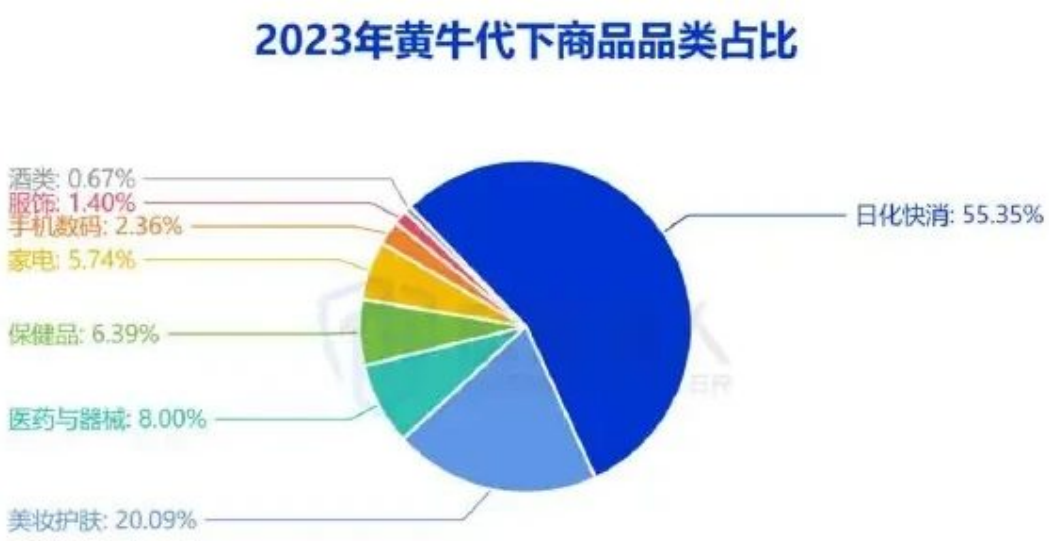
(6) Telegram and the dark web are the main channels for data leakage, accounting for up to 92%. Among the data leakage incidents monitored by Threat Hunter in 2023, more than 92% occurred in Telegram and the dark web, of which

82.26% is concentrated on Telegram, and 10.01% occurs on the dark web. The main reason is that Telegram and dark web channels are concealed.

It is highly reliable and difficult to trace back to threat actors themselves. It is the preferred channel for threat actors to communicate and trade. In addition, Threat Hunter also detected data leakage incidents in code warehouses (such as GitHub, GitLab, Postman, etc.), network disk libraries and other channels.

Marketing activities (Chart 1)

Source: Threat Hunter original report, page 42



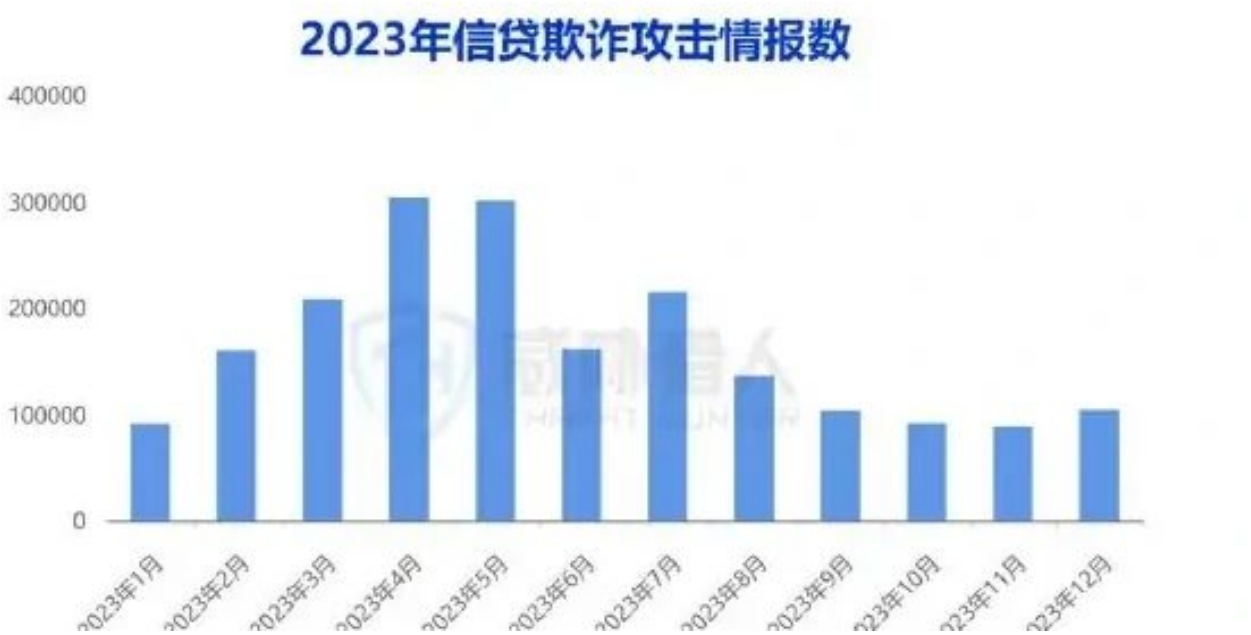
Marketing activities (Chart 2)

Source: Threat Hunter original report, page 42

As of December 2023, Threat Hunter data leakage monitoring intelligence covered nearly 20,000 channels/group chats in Telegram, and risk incidents of citizens' personal information leakage were found in more than 1,700 channels/group chats.

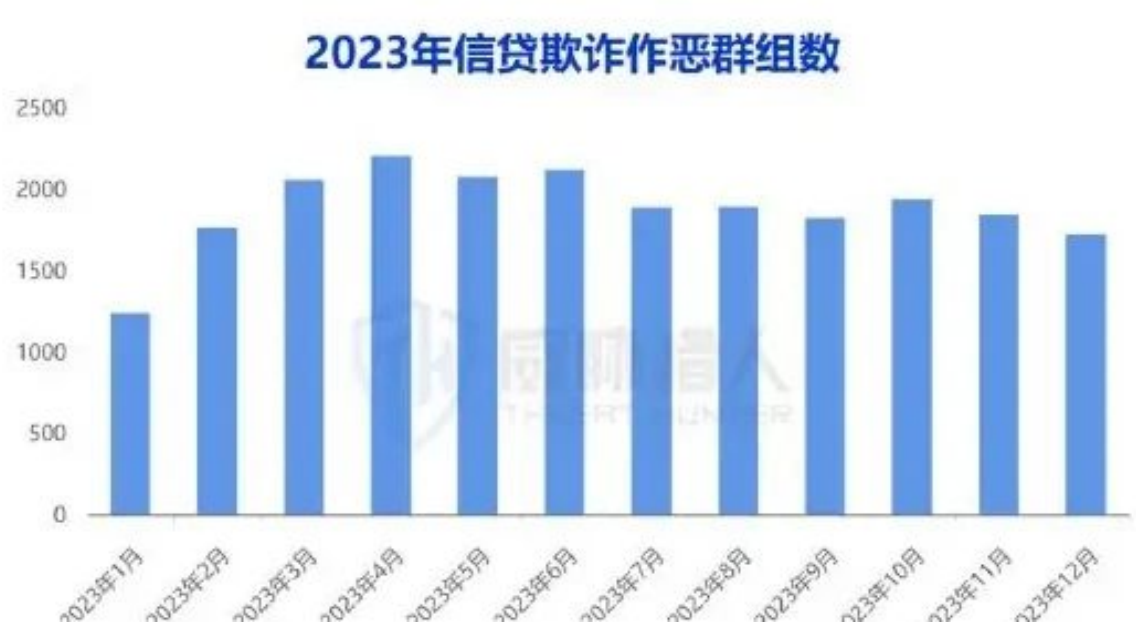
4.3 Analysis of Phishing and Counterfeiting Scenarios in 2023

In 2023, Threat Hunter captured a total of 28,794 cases of phishing websites, involving 234 companies; it captured 1,295 cases of counterfeit apps, involving 67 companies. Such websites and apps gain users' trust and defraud users' personal information and money by imitating normal websites and apps.



Credit fraud (Chart 1)

Source: Threat Hunter original report, page 43



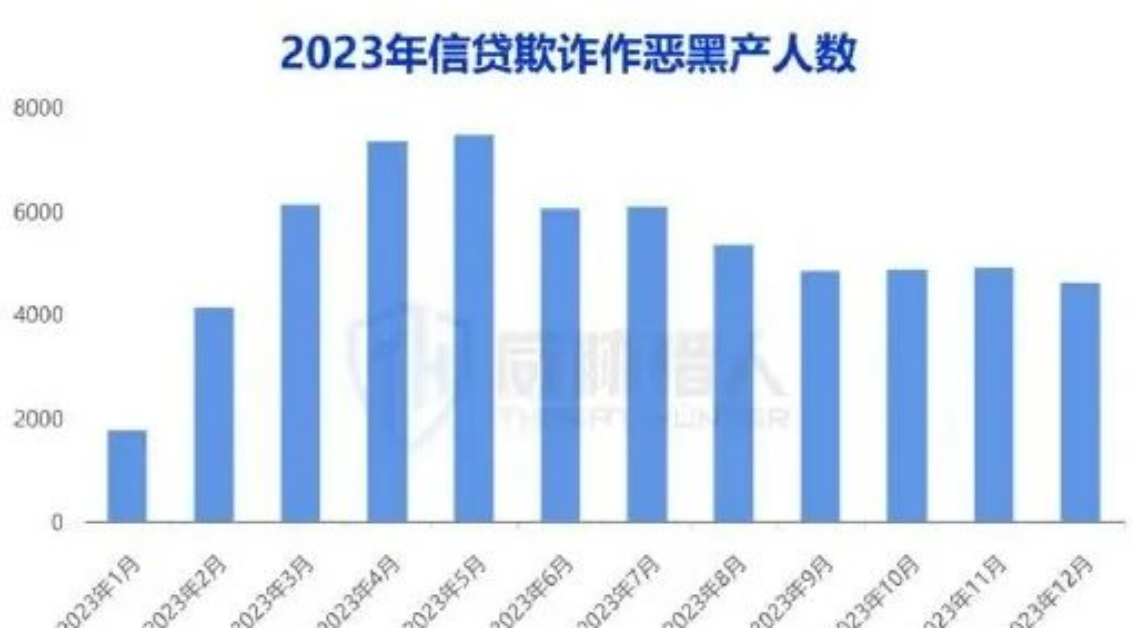
Credit fraud (Chart 2)

Source: Threat Hunter original report, page 43

Threat Hunter researchers analyzed the captured cases and found:

(1) The financial industry suffers the most serious phishing and counterfeiting situations. Whether it is phishing websites or counterfeit apps, the financial industry has become the main target of attacks by threat actors. Since most business scenarios in the financial industry involve capital flows and large transaction amounts, threat actors can often maximize profits without arousing the suspicion of victims. At the same time, in most cases, in order to win the trust of victims as much as possible, threat actors often choose leading companies in the industry to carry out counterfeiting.

(2) The main method of committing crimes is to induce the download of counterfeit financial management and bill-making apps for transfer. 1. Inducing the download of counterfeit investment apps. This type of fraud is relatively hidden. When users register, they need the relevant introducer to provide the registration code to successfully register.



Credit fraud

Source: Threat Hunter original report, page 44

The general process of conducting malicious activity is as follows:

1. threat actors achieve precise customer acquisition through technical means. The target customer group is generally high-income people with a certain amount of deposits;

2. The introducer (“financial management/investment/analyst” in the words of threat actors) induces customers to download the designated app by exaggerating financial management income

Conduct financial management or investment;

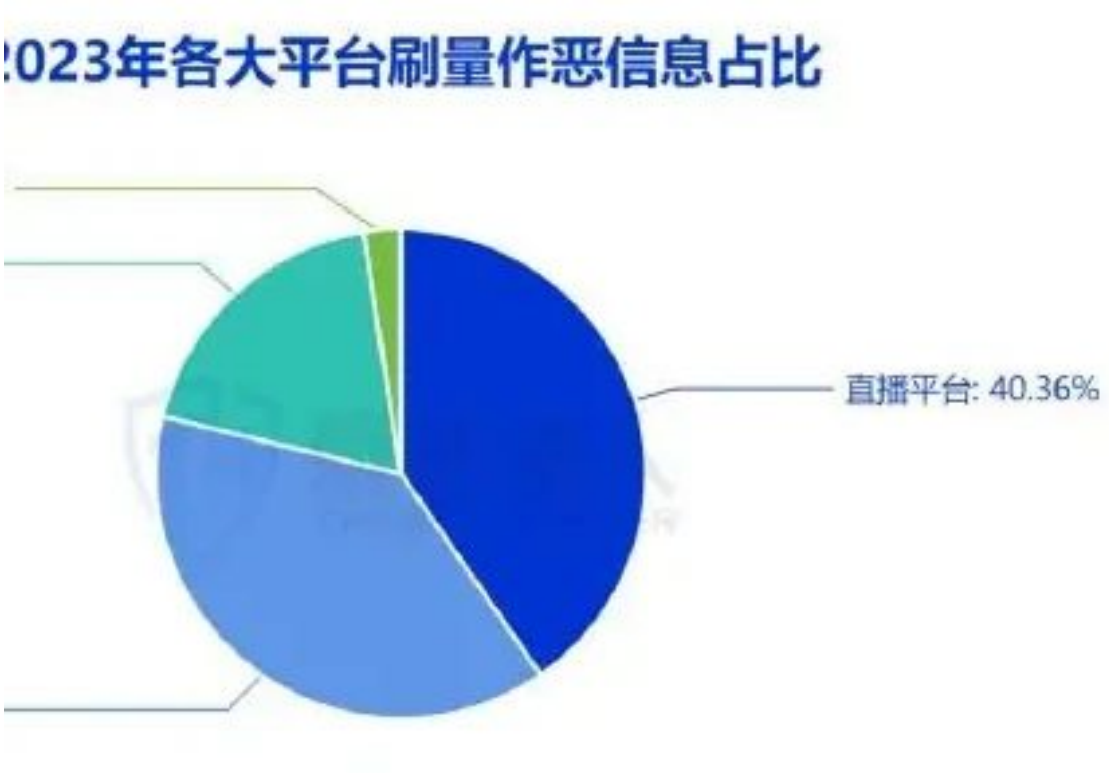
3. Users make short-term, multiple financial investments and receive a certain amount of income each time;

4. The analyst once again induces the user to increase investment in financial management (investment), accumulating a certain amount to lock the user's account;

5. The customer service will then guide the user to recharge and unfreeze the user account. Until the user stops recharging, the platform will "run away" directly.

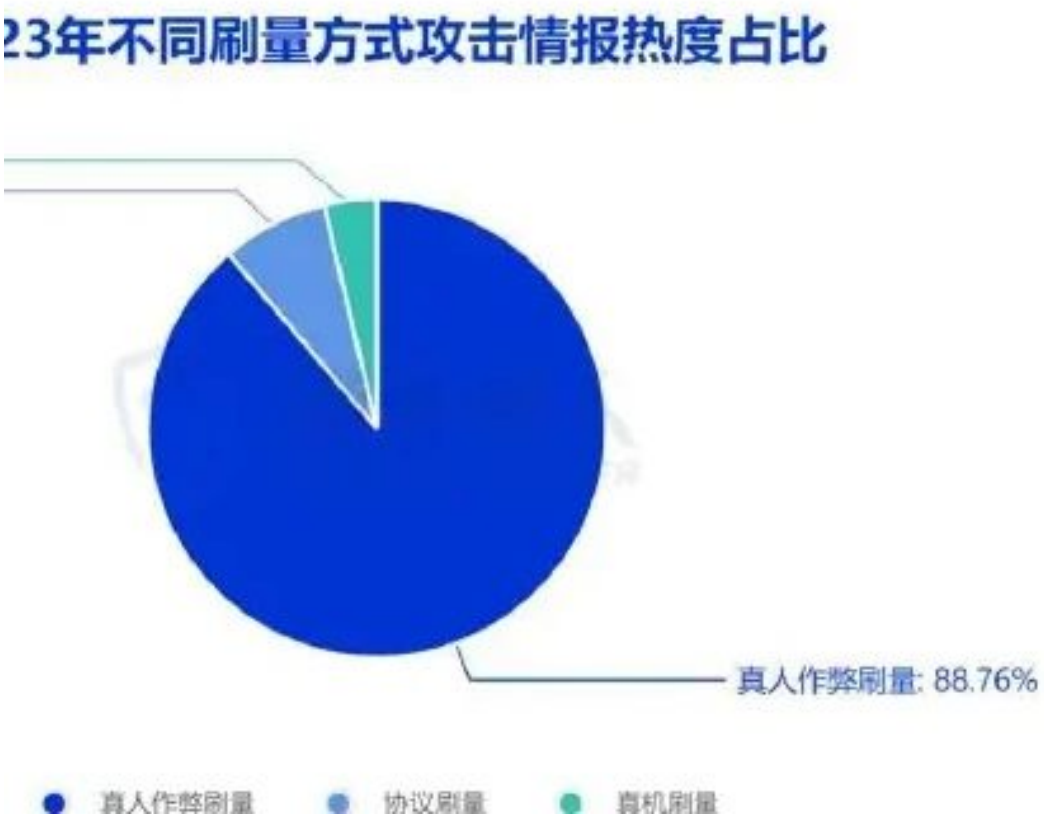
2 Inducing the download of a counterfeit e-commerce fraud app. This counterfeit type appears to be an app that counterfeits an e-commerce platform. After users install the app, they will find that the app is actually a counterfeit social platform app, and then embeds an H5 interface (that is, the fraud system) for fraud. Users need to use the invitation code provided by the upstream to register an account and enter the relevant traffic manipulation system.

The routine of conducting malicious activity is roughly as follows:



Content brush (Chart 1)

Source: Threat Hunter original report, page 46



Content brush (Chart 2)

Source: Threat Hunter original report, page 46

1. The manipulate order system requires users to recharge a certain amount to receive orders. The more the recharge amount, the higher the user's level.

The higher the number of daily orders received and the amount returned from traffic manipulation orders. This model will induce users to continuously recharge. When the recharge reaches a certain level, the account will be frozen.

2. When the user seeks customer service to unfreeze the account status, the customer service will guide the user to recharge more money to resolve the account abnormality before withdrawing money.

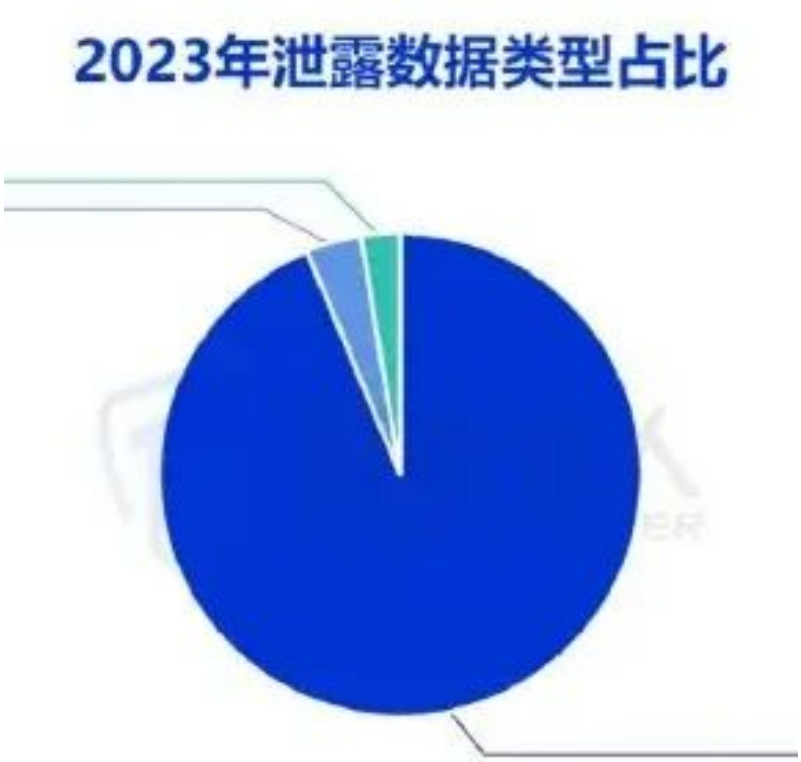
3. After the user does not recharge or discovers an abnormality on the platform, a large amount of the user's funds have been transferred by threat actors, and the platform will also "run away"

road".

Summary

In 2023, the cybercrime ecosystem malicious activity situation became more and more serious. The number of cybercrime operators and the level of malicious resources have shown an upward trend for two consecutive years. The ways for cybercrime ecosystem to obtain malicious resources are more hidden. Whether it is attack resources, malicious methods or malicious activity scenarios, there have been huge changes. The offensive and defensive confrontation of threat actors has also become a great challenge for various enterprise platforms. Judging from the Internet cybercrime ecosystem trends in 2023, companies need to focus on the following issues:

1. In terms of attack resources, the overall resource level of cybercrime ecosystem increased significantly in 2023, and the application method will be more efficient and covert.



2023 Data leak scenario analysis

Source: Threat Hunter original report, page 49

In 2023, domestic malicious phone numbers increased by 15.44% compared with 2022, the number of risky IPs increased by 88.47% compared with 2022, and the number of money laundering bank cards increased by 133.74% compared with 2022.

There are also new trends in applications, such as card issuance platforms becoming one of the mainstream channels for threat actors to deliver high-value code-encrypted mobile phone cards;

threat actors' behavior of maliciously using normal user IPs by implanting Trojans has become more rampant. This kind of "good and bad shared" IPs are more likely to escape corporate fraud controls.

2. In terms of attack technology, the application of AI technology has greatly improved attack efficiency, and the head cloud mobile phone platform is showing an industrialization trend.

2023 Data leak scenario analysis

Source: Threat Hunter original report, page 50

In 2023, AI technology will be used in multiple scenarios of network security, and the in-depth application of AI technology has also aroused the covetousness of a large number of threat actor groups. Many groups of threat actors use AI technologies such as text generation, photo activation, and face replacement to carry out attacks and further commit fraud, including connecting AI robots to automatically generate chat phrases in social scenarios, using AI to forge videos to bypass face verification, etc.

In 2023, the number of platforms providing cloud mobile phone services will continue to increase, and leading cloud mobile phone platforms have shown an industrialization trend. In addition to providing cloud mobile phone services, such platforms will also provide supporting attack tools, such as proxy IP services, machine modification tools, positioning modification tools, Hook frameworks, etc., which greatly improve the efficiency of threat actors' attacks.

3. In terms of attack scenarios, more covert attack methods have emerged in order to evade corporate fraud-control systems.

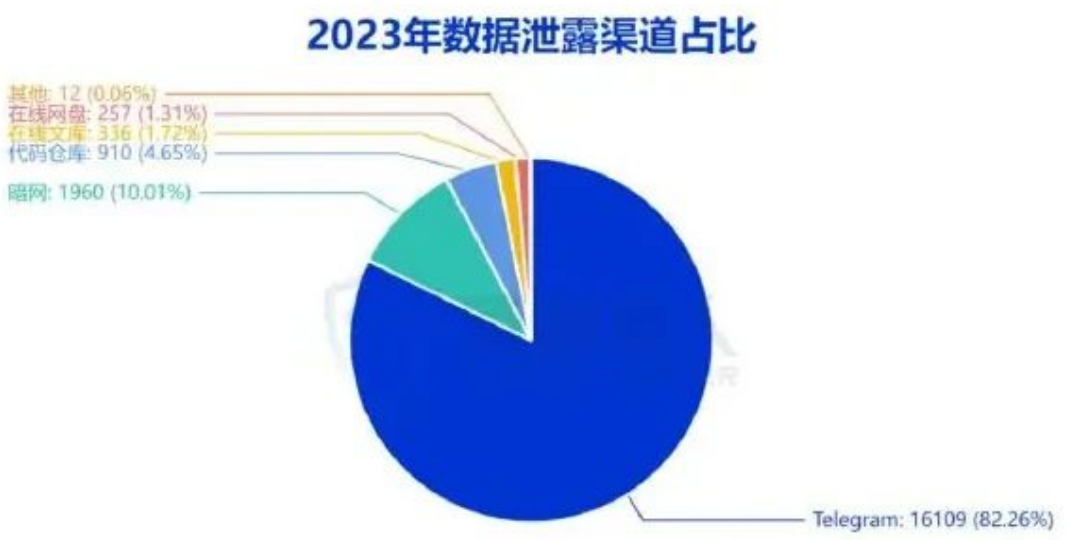
In terms of marketing fraud scenarios, Threat Hunter researchers in 2023 discovered that cybercriminal groups have launched a more complex and secure crowdsourcing release channel in order to avoid monitoring and fraud controls of the crowdsourcing platform. Although this "private domain" of the crowdsourcing platform increases execution time and operating costs, its concealment makes the platform's monitoring and fraud controls much more difficult.

Regarding data leakage scenarios, Threat Hunter researchers found that among data transaction times in citizen personal information leakage incidents, the number of incidents that occurred on

non-working days (weekends and holidays) was as high as 31.21%, and the number of incidents that occurred at night (18:30 to 09:30 the next day) accounted for as much as 51.88%.

Nighttime and non-working hours are when corporate defenses are weakest. It is difficult for most companies to quickly sense and respond in a timely manner when a data breach occurs, so that they miss the best response opportunity, which has a significant impact on corporate funds, brand reputation and business competition.

(如 GitHub、GitLab 、Postman 等）、网盘文库等渠道也监测到了数据泄露事件。



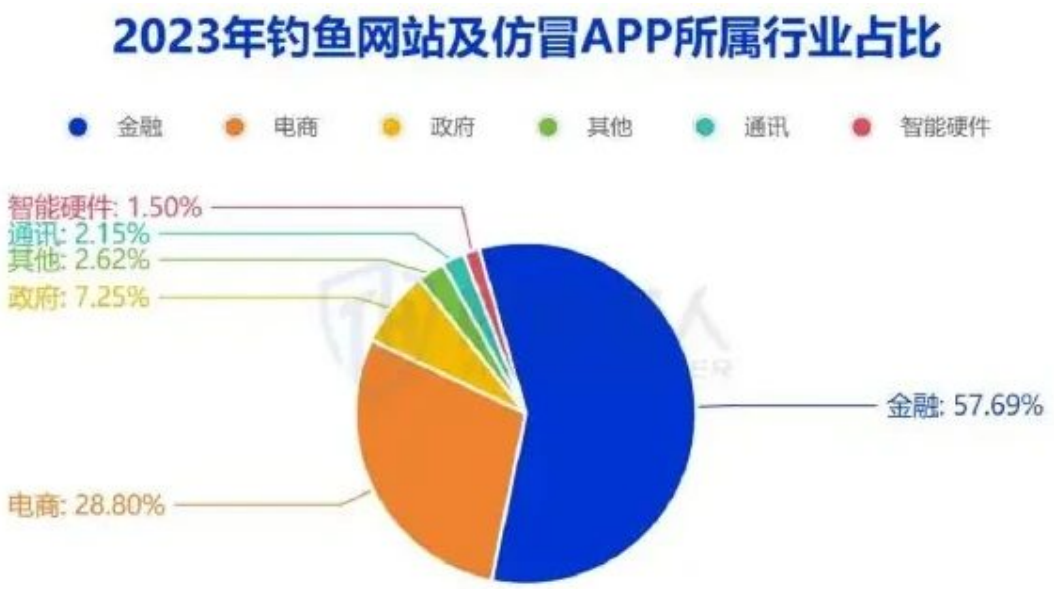
2023 Possibilities analysis

Source: Threat Hunter original report, page 51

In recent years, cybercriminal groups have continuously optimized attack resources and iterated attack technologies to ensure sustained and efficient profits. The increasingly severe cybercriminal groups attack and defense situation also means that various enterprise platforms have a certain lag in sensing cybercriminal groups' attack behaviors.

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. In addition, enterprises also need to realize that the confrontation with external threat actors is dynamic and continuous. They can rely on cybercrime ecosystem intelligence data based on multi-channel monitoring of the entire network to extract cybercriminal groups attack patterns and resource characteristics, match them with abnormal traffic in the enterprise's business, quickly identify risks and carry out targeted defenses.

There is a long way to go to fight cybercrime ecosystem. With the help of external "threat intelligence", enterprises can comprehensively and timely perceive the trajectory and trends of cybercriminal groups, accurately attack cybercrime ecosystem in the increasingly severe cybercrime ecosystem risk landscape, and better protect their own business security.



2023 Possibilities analysis

Source: Threat Hunter original report, page 52