THREAT HUNTER RESEARCH

2022 Cybercrime Ecosystem Research Report

A review of how cybercriminal supply chains, attack resources and defensive priorities evolved during 2022.

Original publication: 2023-03-17
Research team: Threat Hunter Research Team
Source report: 52 pages

Original report text

This text version is reconstructed based on the 52-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

“There are over 2 million practitioners, the average age is 23 years old, and the market size is as high as 110 billion.” This is a statistical data from the Internet Society of China on the “cybercrime ecosystem market size”.

Driven by huge profits, cybercrime operators are wandering crazily on the edge of supervision. Various attack resources of threat actors are highly market-oriented and modular. Gangs at different levels of the industrial chain have clear division of labor and tight cooperation. The cybercrime ecosystem chain is constantly escalating in its confrontation with all parties, and many companies are forced to get involved in the cybercrime ecosystem whirlpool.

Only by "knowing ourselves and the enemy" can we break the offensive and defensive deadlock and promote effective governance. The cybercrime ecosystem chain has always been the focus of Threat Hunter's research. Threat Hunter released the "2022 cybercrime ecosystem research report" (hereinafter referred to as the "Report"), which objectively presents the development trend of cybercrime ecosystem in 2022, conducts an in-depth analysis of attack resources used by cybercriminal groups, technologies, and scenarios, and proposes risk prevention and control ideas.

Development status of cybercrime ecosystem

1. Development status of cybercrime ecosystem in 2022

Statistics from the "Report" show that the domestic cybercriminal groups will still be very developed in 2022, mainly as follows: larger scale, clearer industrial chain structure, more efficient attacks, and wider coverage of scenarios.

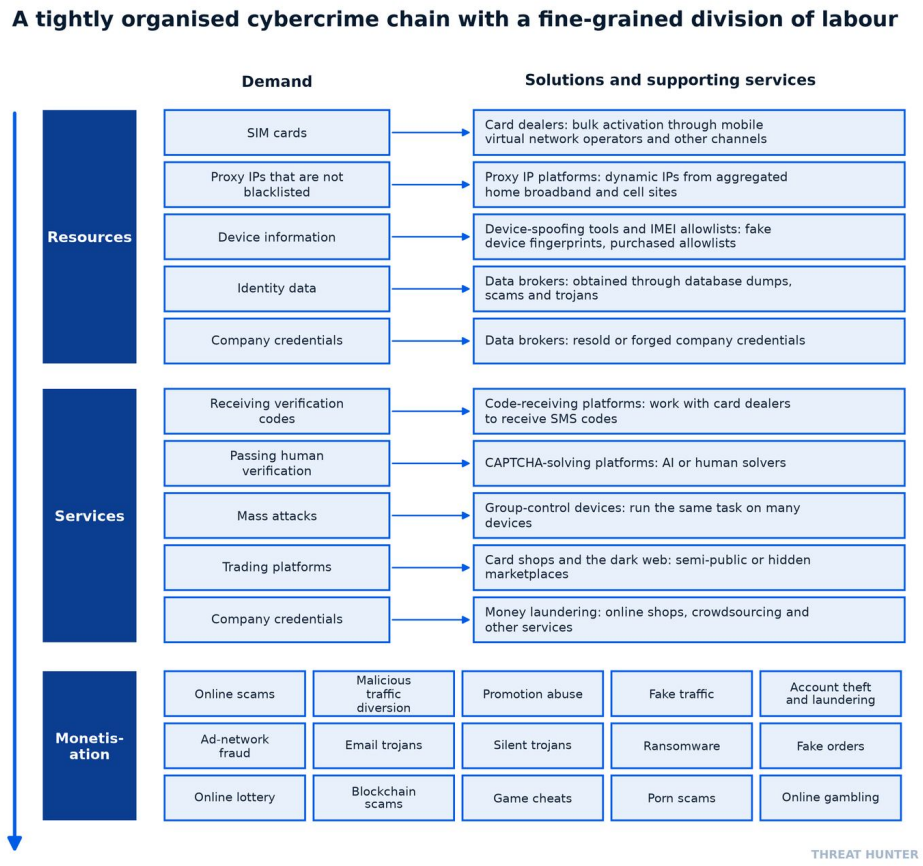
1.1 More than 800 million pieces of cybercrime ecosystem related information, the scale of cybercriminal groups will still be huge in 2022

In 2022, the Threat Hunter intelligence platform monitored more than 800 million pieces of cybercrime ecosystem-related intelligence, and the scale of threat actors is still very large. The overall structure of the cybercrime ecosystem chain in 2022 can be divided into three levels: resources, services, and realization according to the supply and demand relationship, and this is used to distinguish the upstream, middle, and downstream of the industry chain:

Resource layer: As the upstream, it controls the underlying basic resources for cybercrime ecosystem malicious activity;

Service layer: As a midstream, it integrates upstream resources and its own technology to provide various service support for downstream attacks;

Realization layer: As the downstream, that is, the actual threat actors attack group, attack the business and ultimately realize the realization of benefits.

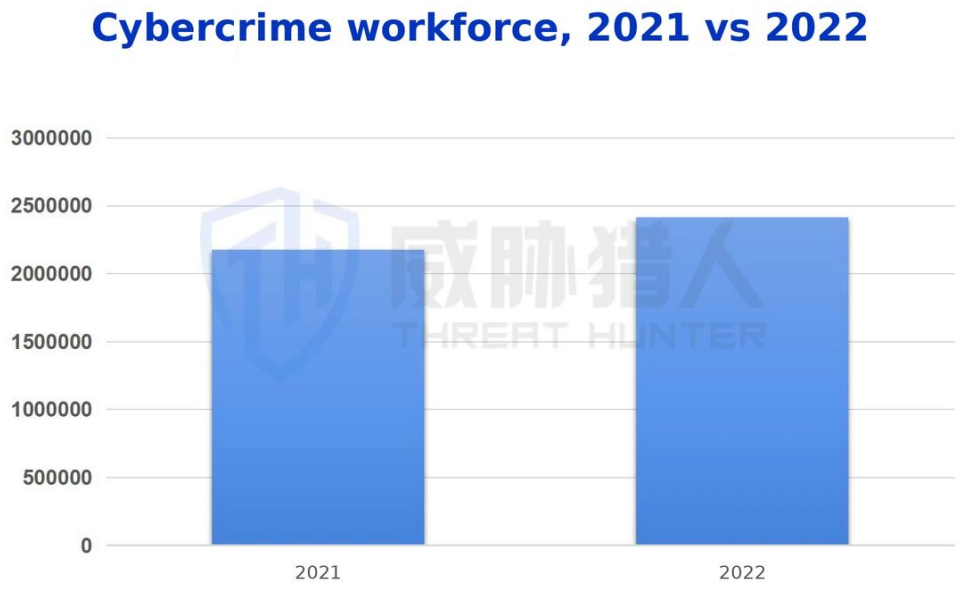


A tightly organised cybercrime chain with a fine-grained division of labour

Source: Threat Hunter original report, page 5. Redrawn in English from the original figure.

1.2 The number of cybercrime operators will be wider in 2022, an increase of 10% compared with 2021

The number of threat actors in 2022 will be wider, and the number of cybercrime operators in 2022 increased by about 10% compared with 2021.



The cybercrime workforce grew by about 10% in 2022 compared with 2021

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

1.3 Due to the continued impact of the "Card Break Operation", the number of new threat-actor resources decreased in 2022

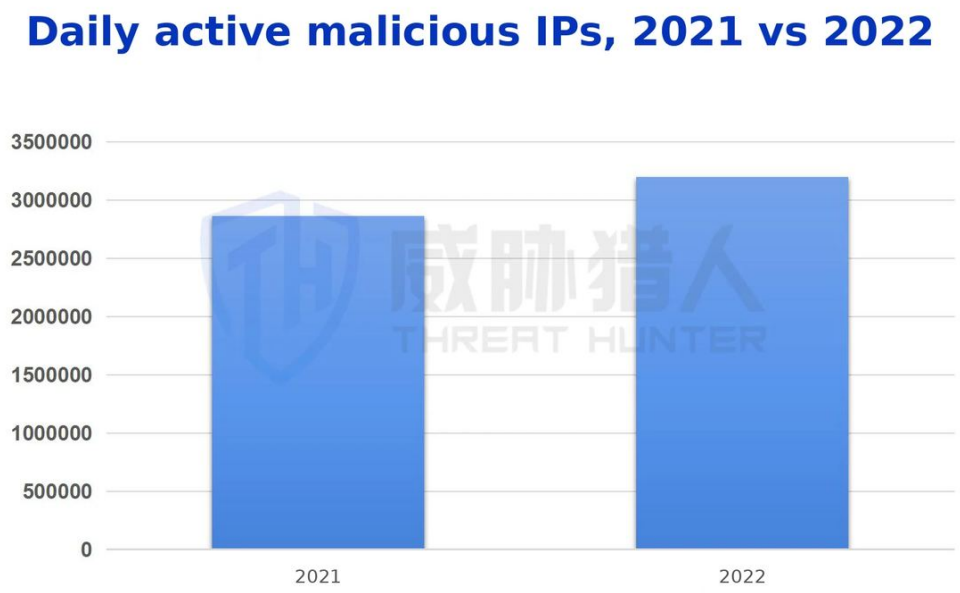
illicit SIM cards are very important the cybercrime ecosystem resources. Whether it's promotion abuse or fake likes, etc., threat actors need to hoard a large number of accounts, and the main source of accounts is illicit SIM cards registration. In 2022, the "card disconnection operation" continues to heat up, and it is increasingly difficult for threat actors to obtain domestic traditional black phone numbers. The increase in traditional black phone numbers in 2022 has dropped by about 26% compared with 2021.



New traditional illicit SIM cards, 2021 vs 2022

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

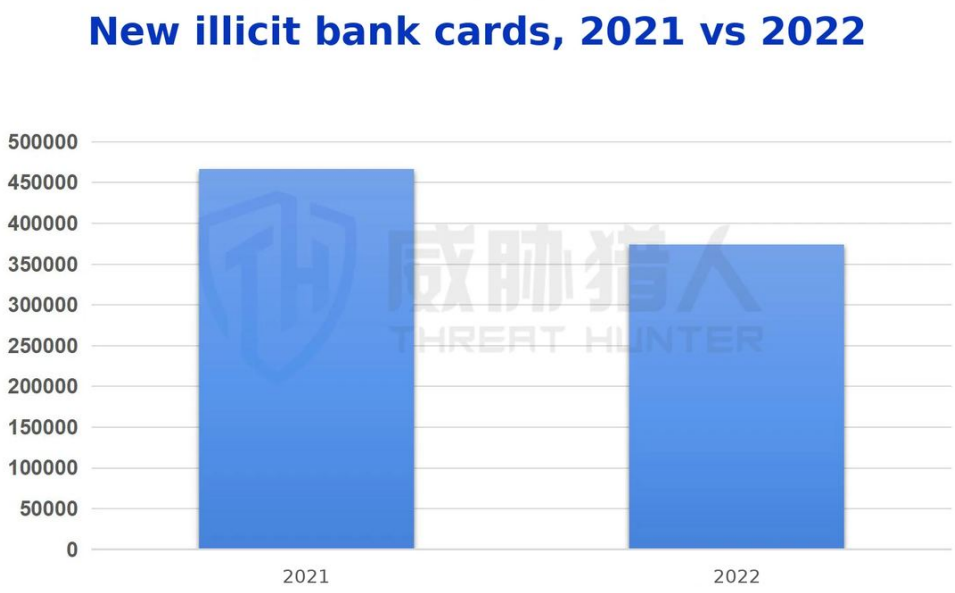
Black IP is also one of the important the cybercrime ecosystem resources. cybercriminal groups use a large number of black IP to bypass the enterprise's IP-based fraud controls and hide the attacker's real IP. The overall black IP resources will not change much in 2022, and the number of daily active black IPs increased by about 12% compared with 2021.



Daily active malicious IPs, 2021 vs 2022

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

Black bank cards are an important resource for money laundering in illegal activities such as online gambling, pornography, and fraud. Threat Hunter intelligence platform monitoring found that the number of new black bank cards in 2022 has dropped by about 20% compared with 2021. Research infers that it is mainly due to the continued intensification of the "card disconnection operation" in 2022 that banks have achieved certain results in the management of black bank cards.



New illicit bank cards, 2021 vs 2022

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

1.4 The threat actors attack service is divided into three major modules: "over-identity", "multi-identity", and "batch"

Threat Hunter conducted in-depth research and summary on the midstream service layer of the industry chain, and divided the attack service into three modules: "over-identity", "multi-identity" and "batch", each of which involves multiple attack technologies.

Overidentity: Using forged identities, faces, etc. to bypass platform authentication, you can register false accounts and participate in platform business and activities normally;

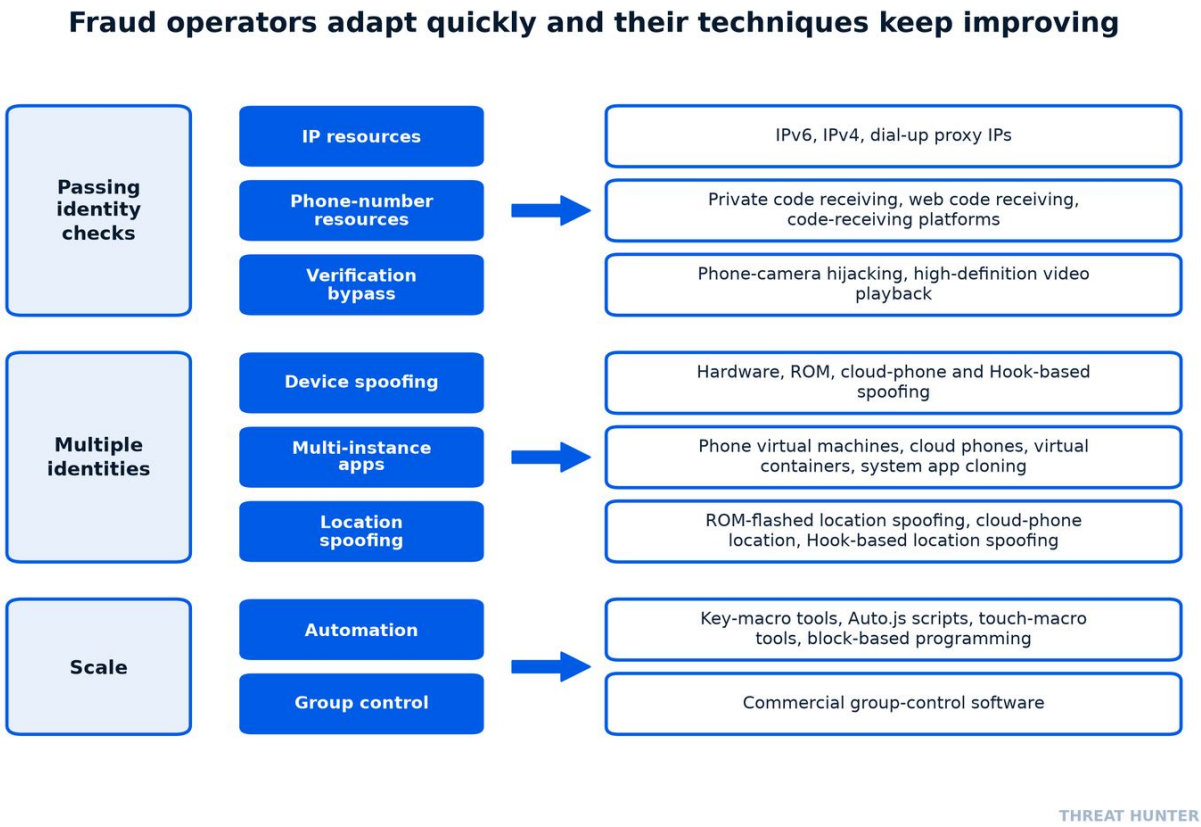
Multi-identity: Use techniques such as multi-opening, machine modification, and positioning modification to forge multiple "normal" devices, thereby bypassing the platform's restrictions on single identity;

Automation: Use automated scripts or group control tools to complete registration, login, click and other business operations in batches.

Note: A detailed analysis of attack resources used by cybercriminal groups and technologies in 2022 will be explained in detail in Chapters 2 and 3.

1.5 The cybercrime ecosystem malicious activity situation is still severe, involving six major attack scenarios such as promotion abuse and false volume traffic manipulation.

In 2022, the scale of cybercriminal groups will not decrease, and the crime situation remained serious. Threat Hunter conducted in-depth research on the key attack scenarios of cybercrime ecosystem in 2022, such as promotion abuse, false traffic manipulation, and data leakage. Among them, promotion abuse is still the main attack scenario of cybercrime ecosystem. In addition, the traffic manipulation industry chain continues to evolve, and new "premium account" traffic manipulation quietly appears.



Fraud operators adapt quickly and their techniques keep improving

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

Note: More cybercriminal groups attack scenario analysis will be explained in detail in Chapter 4.

cybercriminal groups attack resource analysis

2. Analysis of attack resources used by cybercriminal groups in 2022

2.1 The increase in illicit SIM-card resources will fluctuate greatly in 2022

According to Threat Hunter's observation, cybercriminal groups provide sufficient "ammunition" for malicious purposes in various risk scenarios through traditional illicit SIM cards, interception cards, foreign SIM cards, etc., which reflects the extremely strong resistance and vitality of cybercrime ecosystem.

2.2.1 Traditional illicit SIM cards

Key attack scenarios for the cybercrime ecosystem in 2022

Attack scenario	Targets
Marketing fraud	All industries
Fake traffic	Social media, media and news
E-commerce fraud	E-commerce
Credit fraud	Finance
Online money laundering	Banking, payments and similar industries
Data leaks	All industries

Key attack scenarios for the cybercrime ecosystem in 2022

Source: Threat Hunter original report, page 10. Table re-typeset in English from the original.

Traditional illicit SIM cards refer to abnormal real-name mobile phone SIM cards. There are various channels, including corporate anonymous cards, historical IoT cards, communication virtual cards, etc. The main feature is that they are "fixedly held by threat actors during the life cycle", that is, no matter which platform you register for during this period, any behavior you perform can be judged as malicious.

The supply of traditional illicit SIM-card resources in 2022 is not stable. The number of new traditional illicit SIM cards every month is as shown in the figure below:

According to analysis by Threat Hunter intelligence experts, there are two main reasons for the large fluctuations in increments:

1. Due to the continuous impact of the "Card Disconnection Campaign", card dealers are unable to issue new cards in batches through channels such as in-store sales halls. Many card dealers only

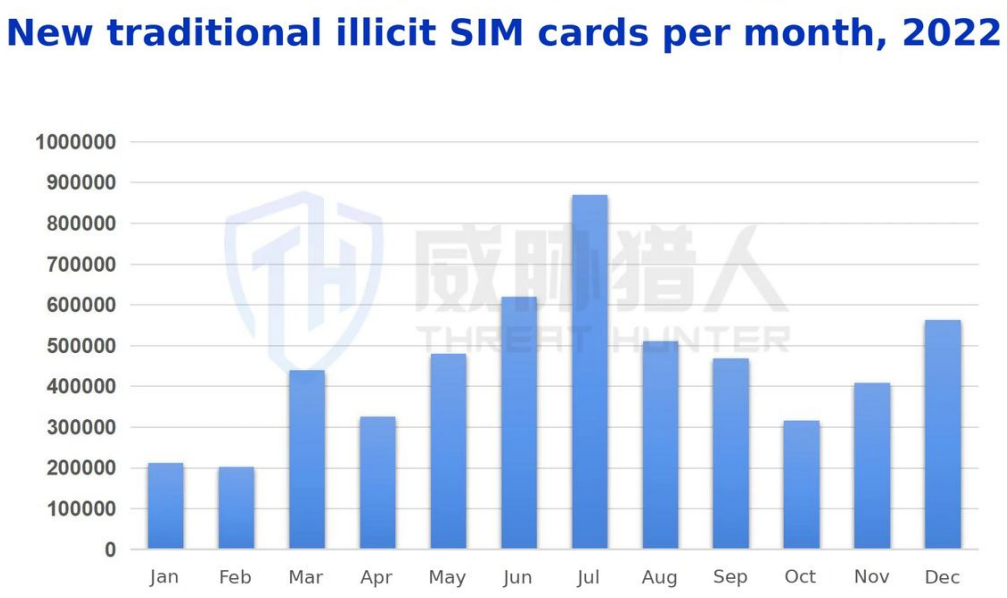
Can use old cards to launch some new businesses;

2. The most important connection channel for traditional illegal phone number cards, the number receiving platform, was attacked by the police in 2022, and the platform ran away, etc.

The influence of practical factors has intensified the fluctuation in new illicit SIM cards.

Faced with the heavy blows of regulatory platforms, threat-actor groups have also emerged with various coping strategies:

1. Some card merchants have discovered new channels to issue cards in batches (such as using cloud platform number privacy protection services). Therefore, some



New traditional illicit SIM cards per month, 2022, with large month-to-month swings

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

The number of cards supplied increased during this period;

2. The SMS verification-code receiving service is affected by a variety of practical factors. Card merchants have gradually gathered into a very small number of leading SMS verification-code receiving services. The services of these platforms

Weapons are usually hosted outside mainland China and are more difficult to take down;

3. In order to avoid being easily discovered, more and more card dealers adopt private docking. The private docking code in 2022

The method gradually changed from "group code access" to "web page code access".

Group access codes: Groups established by sellers in messaging apps are easily detected and banned, so code access groups need to be frequently established or changed, and group access codes are relatively unstable;

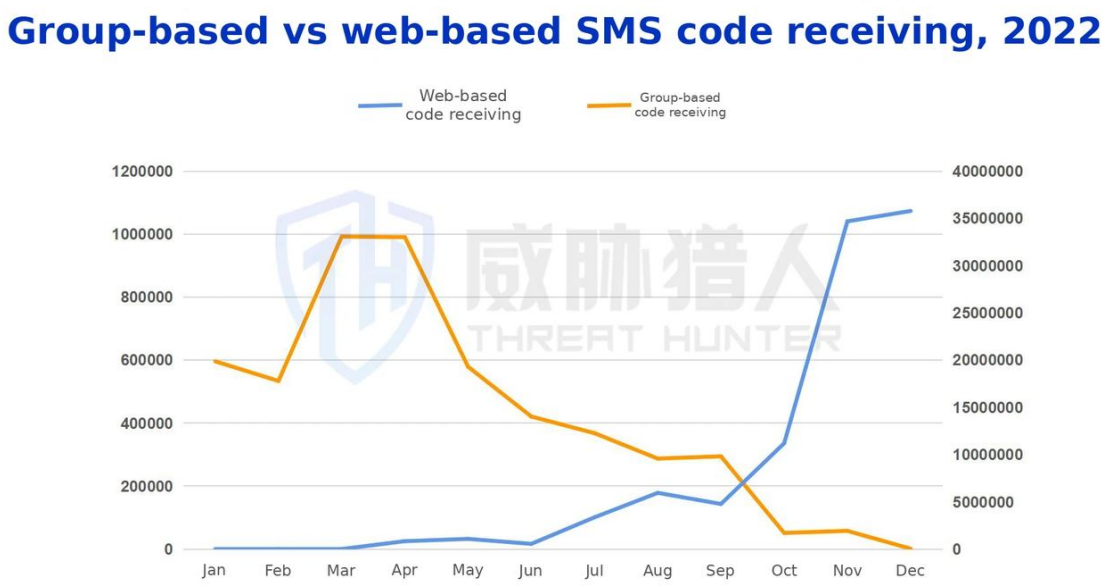
Web page code reception: There is a specific group of threat actors responsible for developing transcoding software and websites. Sellers can generate exclusive links through the software and provide them to buyers for receiving text message content (commonly known as code reception rooms). Web page code reception is more convenient and hidden. The principle is as follows:

The following is a comparison of the trends of the two code collection methods in 2022. It can be seen that the scale of web code collection continues to grow, while group code collection continues to decline. By the end of 2022, the number of verification codes received by web page access codes every month has reached tens of millions, while group access codes have almost disappeared.

2.2.2 Interception card

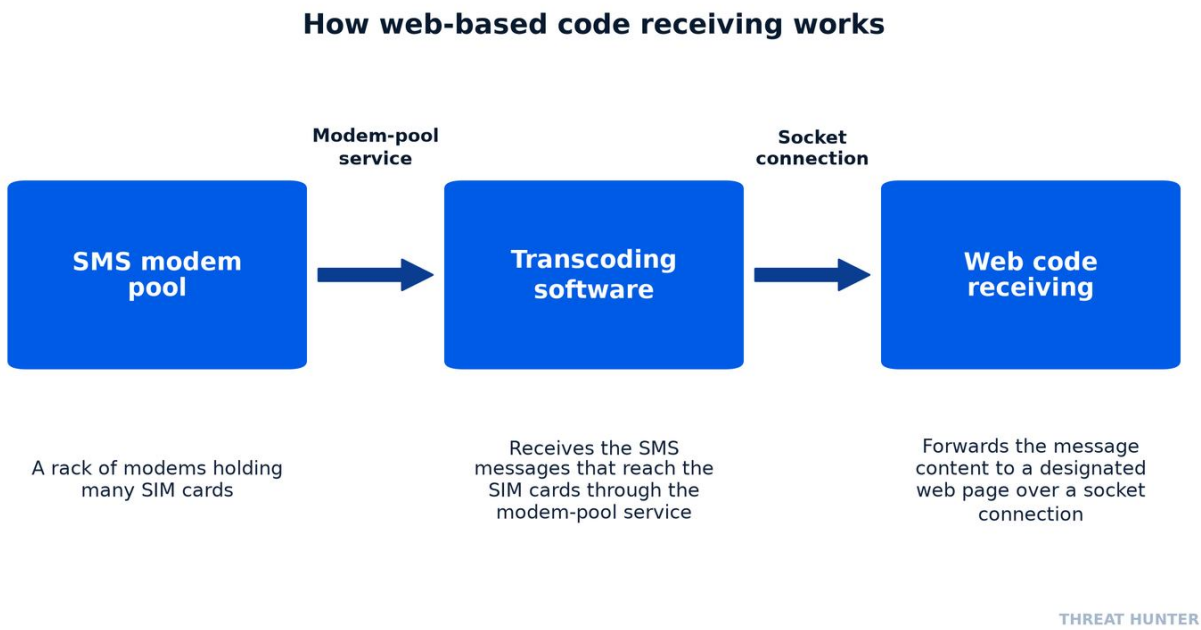
The main feature of the interception card is that "the phone number is held by a natural person", that is, the "real-name card". It refers to leaving a backdoor or implanting a Trojan horse on a mobile device with communication functions to intercept the content of text messages received by normal users' mobile devices and use them to carry out malicious activities. We call it "interception card" for short.

Threat Hunter's investigation found that the number of interception cards in the first half of 2022 was very small, mainly due to the collective withdrawal of interception card platforms in early 2022. Starting from July 2022, multiple new interception card platforms appeared one after another and continued to be active. Therefore, the number of interception cards increased significantly in the second half of 2022.



Group-based vs web-based SMS code receiving, 2022: web-based receiving overtook group-based receiving

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



How web-based code receiving works

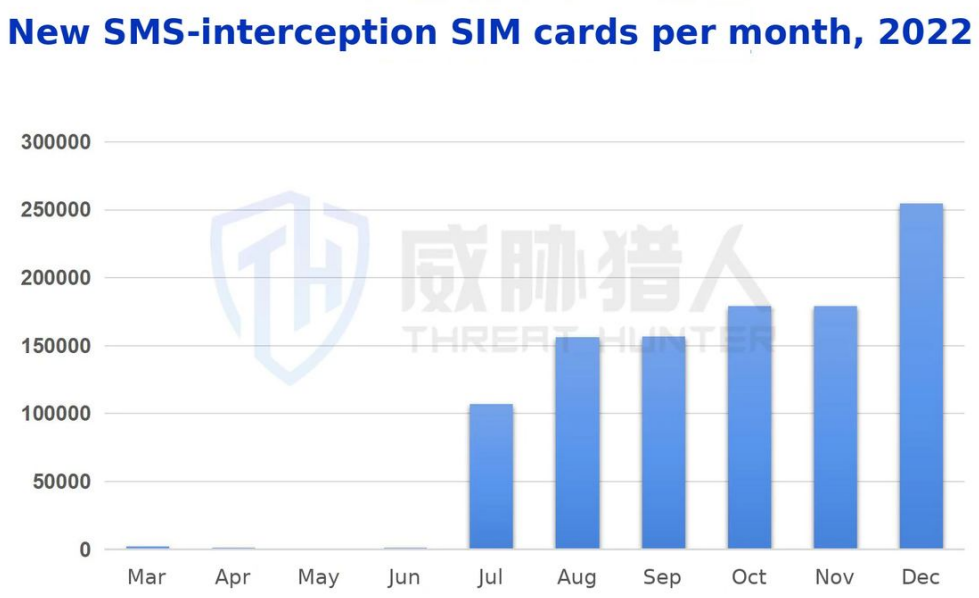
Source: Threat Hunter original report, page 14. Redrawn in English from the original figure.

2.2.3 Foreign illicit SIM cards

Both the code-receiving platforms and the card sources for foreign illicit SIM cards are located outside mainland China, so these cards were not affected by the special crackdown. Their number is expected to stay relatively stable throughout 2022. By geography, foreign illicit SIM cards are mainly concentrated in the United States, Canada, Hong Kong, Southeast Asia and other regions.

2.2 In 2022, the daily activity of black IPs will be stable at around 3 million, and the proportion of black IPs in home broadband will rank first.

The number of black IP resources will be relatively stable in 2022, with the number of daily active black IPs stable at around 3 million. Threat Hunter researchers analyzed the main types of black IPs (excluding data with unknown IP types) and found that home broadband types accounted for the highest proportion of black IPs, exceeding 85%; followed by enterprise dedicated lines and data centers, accounting for about 6%-8%; while other types of black IPs such as mobile networks and campus networks accounted for only 0.35%.

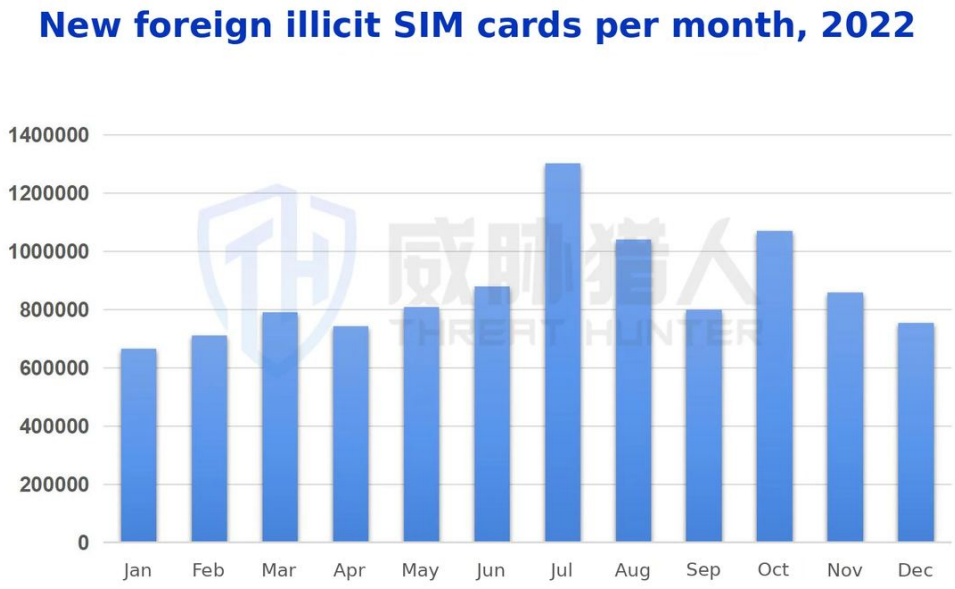


New SMS-interception SIM cards per month, March to December 2022

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

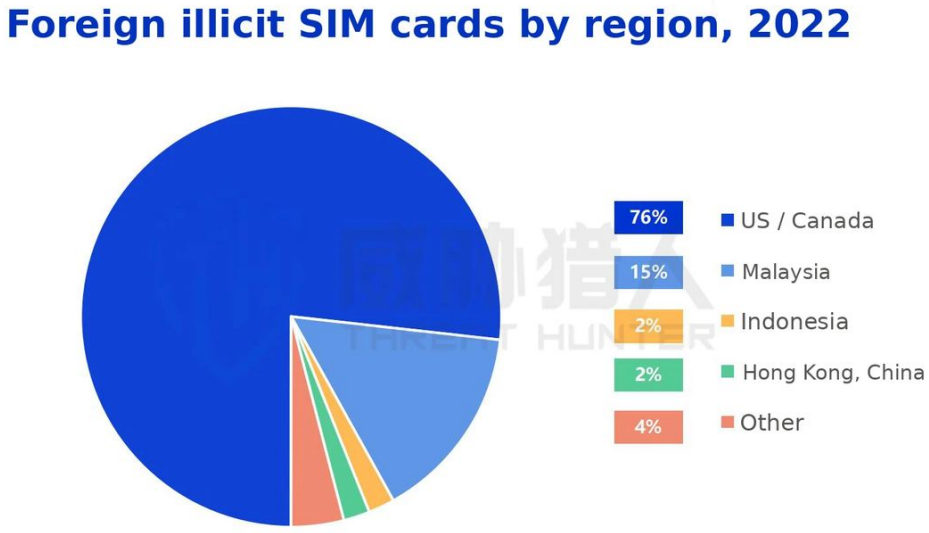
Home broadband: The second dial and dynamic proxy IPs used by threat actors are basically of the home broadband type. They mainly use the principle of "every time the home broadband dial-up is disconnected and reconnected, a new IP will be obtained again." Second dial and dynamic proxy IPs are cheap, large in quantity, and easy to switch, so they have become the first choice black IP resources for large-scale attacks by threat actors.

Enterprise dedicated lines: The number of black IPs of the enterprise dedicated line type has increased in the past year or two. Some black IP resource suppliers apply for enterprise dedicated line IPs through corporate identities and sell them in high-quality pools, exclusive pools, etc. Because these black IPs are expensive and often used by certain groups of threat actors for targeted attacks, their identification is even more difficult.



New foreign illicit SIM cards per month, 2022

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

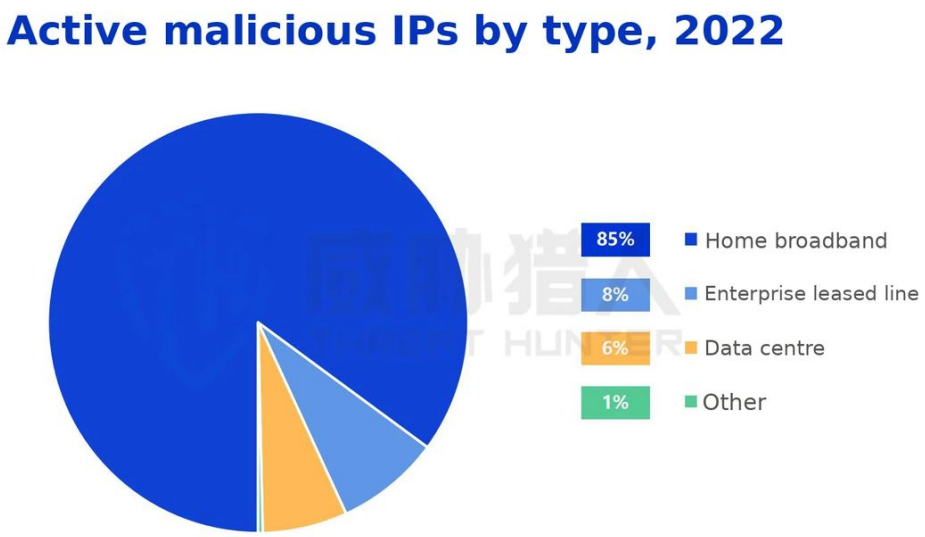


Foreign illicit SIM cards by region, 2022

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

Data center: Data center-type black IP resources are mainly used for promotion abuse scenarios such as flash sales and rush sales. Such scenarios often require IP resources with faster network speeds. Therefore, resource suppliers will choose to rent computer rooms to meet the needs of some threat actors for fast network speed IP resources.

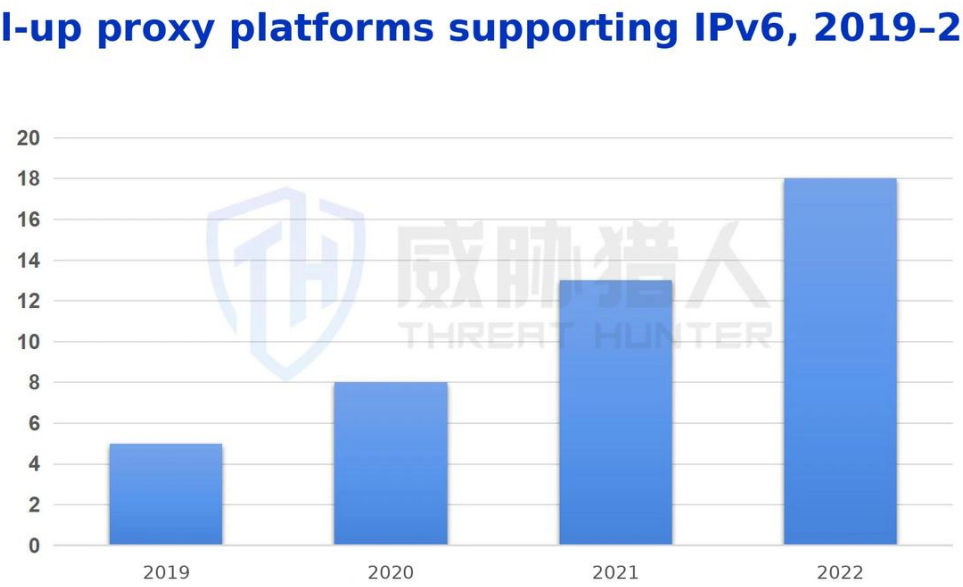
The demand for proxy IP will surge in 2022, and the resource suppliers of black IP will be mainly proxy IP platforms. In 2022, the resource suppliers of black IP will mainly be non-compliant proxy IP platforms and instant dial platforms, of which proxy IP platforms will be the main ones. As major applications begin to display the user IP address, the demand for proxy IP will surge, which will invisibly promote the growth of the number of proxy IP platforms. At the same time, the proxy IP platform is closely connected with the Speed □□Dial platform, and many dynamic proxy IPs are dialed by the Speed □□Dial platform.



Active malicious IPs by type, 2022: home broadband accounts for the largest share

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

IPv6 is becoming more and more popular, and the number of IPv6-enabled dial-up platforms is increasing year by year.



Dial-up proxy platforms supporting IPv6 grew every year from 2019 to 2022

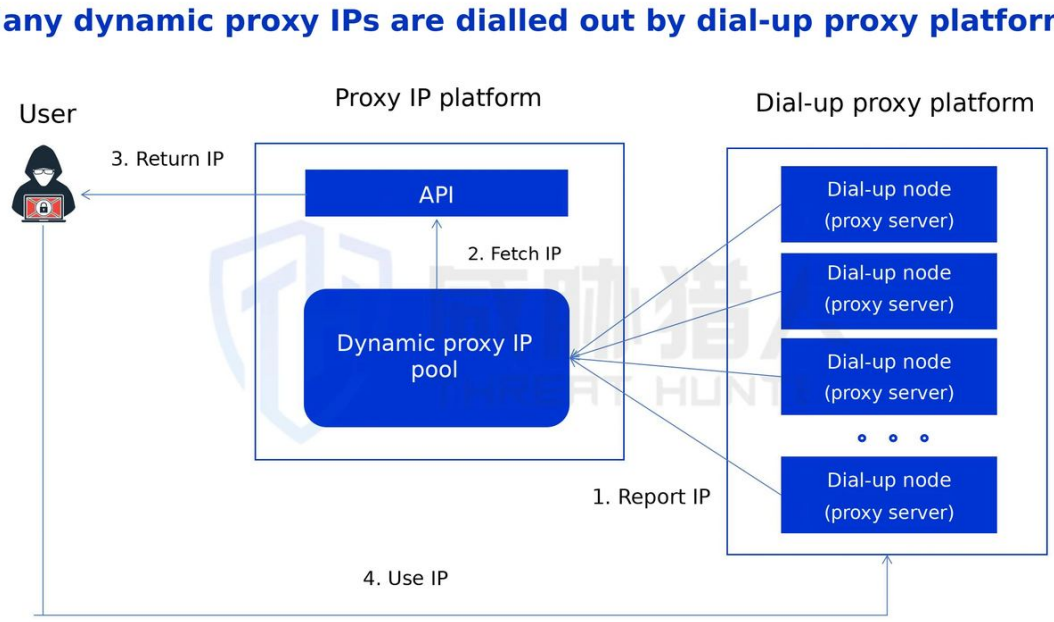
Source: Threat Hunter original report, page 19. Original figure with Chinese text replaced by English.

IPv6 is becoming increasingly popular in the country and continues to have an impact on black IP resource suppliers. At present, although the proxy IP platform does not yet provide proxy IP for IPv6, the second dial platform has provided IPv6-supported seconds since 2021. At the same time, the number of second dial platforms supporting IPv6 is increasing year by year.

Testing and analysis by Threat Hunter intelligence experts for some IPv6-enabled dial-up phones found:

1. Thanks to the fact that the address space of IPv6 is much larger than that of IPv4, the IPv6 address duplication rate dialed by IPv6 seconds is very low.

Attackers can completely use different IP addresses for each attack, which brings new challenges to the identification of black IPs;



Many dynamic proxy IPs are dialled out by dial-up proxy platforms

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

2. Although the IPv6 address dialed by the IPv6 second dialer is different each time, certain rules are still followed in address allocation.

law. Threat Hunter observes the rules of IPv6 address allocation by a dial-up proxy platform, combines it with the captured IPv6 data used by threat actors for analysis, and forms identification rules to form a set of IPv6 risk identification algorithms, which can detect the risk value of IPv6 traffic in business traffic during the active time for enterprises.

With the rapid development and popularization of the Internet, global IPv4 addresses are on the verge of exhaustion. IPv6, as the next-generation IP protocol that replaces IPv4, has huge advantages in the number of IP addresses, security, mobility, service quality, etc. Enterprises need to always pay attention to changes in the supply side of threat actors on the IP resource supply side and adopt response strategies in a timely manner.

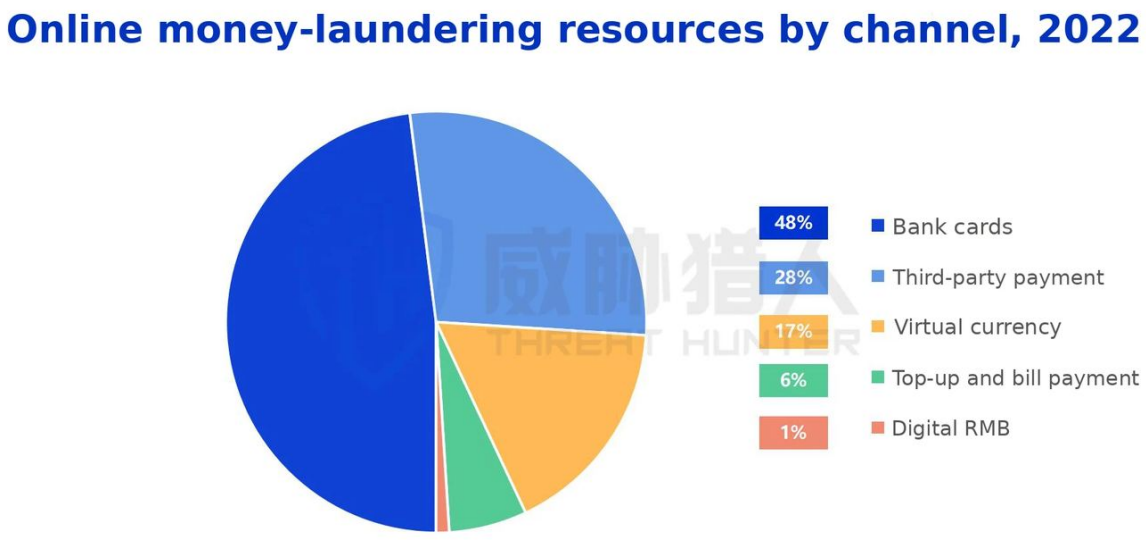
2.3 Bank cards, third-party payment, and virtual currencies have become the main online money laundering resources

According to statistics from relevant departments, the number of illegal gamblers in China currently exceeds 10 million, and gambling-related funds flow out of the country every year exceeding one trillion yuan, seriously threatening national economic security. Focusing on illegal platforms such as online gambling and score-running, Threat Hunter intelligence researchers have discovered through long-term investigation and data analysis that the main channels for online money laundering in 2022 are as follows:

2.3.1 Bank Card

Bank cards are still the most important online money laundering channel, especially for online gambling. From the second half of 2022, black bank cards have shown a rapid upward trend, with monthly new additions exceeding 50,000 during the World Cup.

By comparing the ranking changes in the number of gambling-related cards in banks in the past two years, it was found that 8 of the top 10 banks with the fastest rise in rankings are rural credit cooperatives. It can be seen that with the suppression of major banks, the risk of money laundering of gambling funds has shifted, and bank cards of rural credit cooperatives have gradually been used by gambling platforms on a large scale.



Online money-laundering resources by channel, 2022: bank cards, third-party payment and virtual currency lead

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

2.3.2 Virtual currency

Due to its anonymity and difficulty in tracking, virtual currencies have long been used by threat actors as money laundering and other underground transaction payment channels. In 2022, the active number of virtual currencies used for money laundering will be relatively stable, reaching a peak during the World Cup group stage in November 2022, with monthly active amounts exceeding 50,000.

2.3.3 Recharge and Payment app

threat actors maliciously use the recharge and payment functions of certain apps such as phone bills and electricity bills to complete money laundering by recharging and paying for others at low prices. In 2022, the money laundering method of recharge and payment will be used by more threat actors. Taking the payment of electricity bills as an example, in the second half of 2022, the number of fake accounts used to launder money through the payment of electricity bills has shown a rapid increase.



New illicit bank cards per month, 2022

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

The 10 banks whose share of illicit bank cards rose fastest in ranking over the past two years

	2022 rank	Bank	Rise in rank vs 2021
1	25	Rural credit cooperative, Province A	+34
2	27	Rural credit cooperative, Province B	+33
3	26	Rural commercial bank, City C	+21
4	28	Rural credit cooperative, Province Z	+20
5	16	Rural credit cooperative, Province E	+11
6	14	Rural credit cooperative, Province Y	+10
7	8	Rural credit cooperative union, Province G	+9
8	17	Rural credit cooperative union, Province H	+9
9	24	Rural credit cooperative union, Province K	+4
10	10	A bank in City S	+3

The 10 banks whose share of illicit bank cards rose fastest in ranking over the past two years

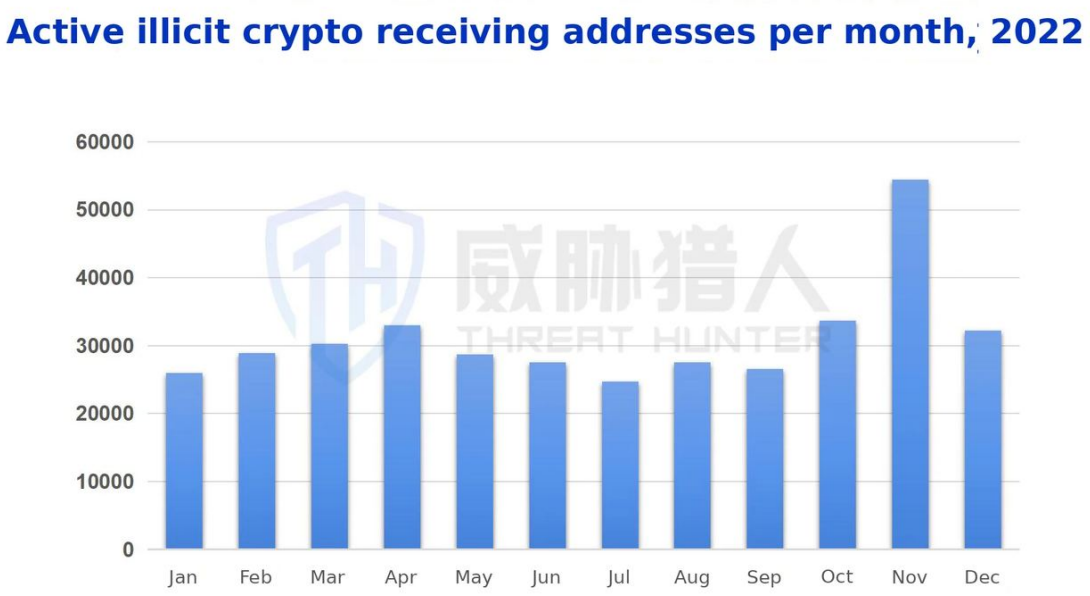
Source: Threat Hunter original report, page 21. Table re-typeset in English from the original.

2.2.4 Digital RMB

As an emerging payment method, digital RMB wallets have been commonly used by online gambling platforms to collect money and launder money since July 2022, showing a clear upward trend.

Digital RMB wallets are mainly divided into four categories. The "fourth category wallet" with the lowest authority is an anonymous wallet. Users can open it with just their phone number. Transfers can be made between anonymous accounts at will, becoming a new recharge method for gambling platforms to bypass payment supervision.

Threat Hunter's investigation found that 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. After transferring gambling funds, cancel the digital RMB account to avoid supervision.



Active illicit crypto receiving addresses per month, 2022

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

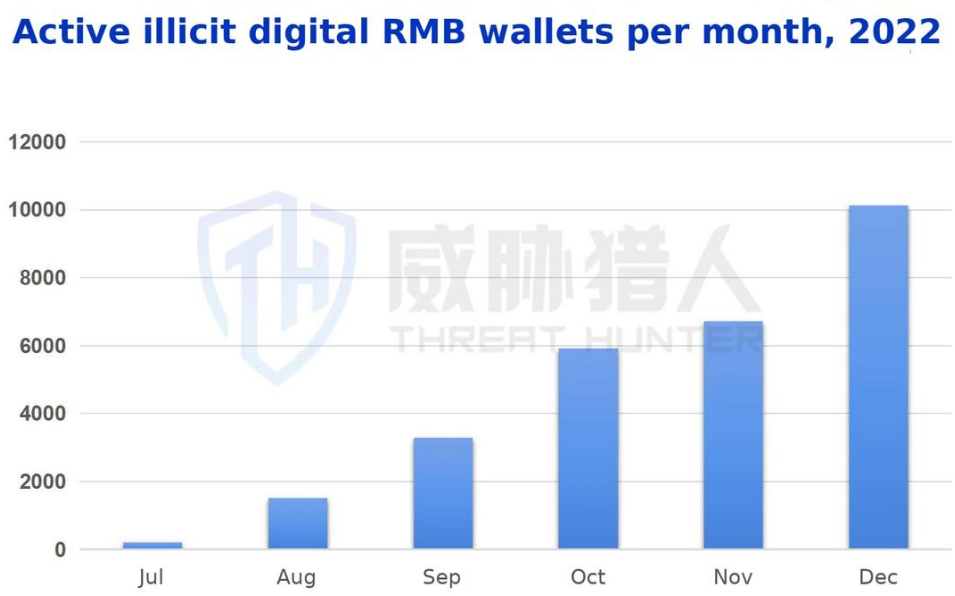
Analysis of cybercriminal groups attack technology

3. Analysis of cybercriminal groups attack technology in 2022



Laundering via proxy electricity-bill payment: activity per month, 2022

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



Active illicit digital RMB wallets per month, July to December 2022

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

When cybercrime ecosystem commits malicious activity, it will use various attack technologies to carry out batch and automated attacks to achieve more profits in a short time. In 2022, the main attack technologies of cybercrime ecosystem include machine modification technology, positioning modification technology, face authentication bypass technology, etc.

3.1 The three major categories of modification technologies are still active, and customized ROM modification technology has become mainstream

Phone modification is an important technical means that threat actors rely on to commit large-scale malicious activity. It mainly refers to using specific technologies to modify the brand, model, serial number, IMEI, MAC address and other device information of the mobile phone, thereby "disguising" it as a new device. threat actors can bypass fraud controls by modifying phones and forging new devices in batches. At present, the types of computer modification tools mainly include: software modification, ROM modification, and hardware modification.

3.3.1 During software modification, the LSPosed framework has become the main modification framework due to its high concealment

Software modification: Software modification has been around for many years. Its core technology is to achieve the modification effect by grabbing functions related to device information and modifying the return value of the function.

Software modification generally uses the Hook framework. Hook frameworks include the XPosed framework and the LSPosed framework. The LSPosed framework has emerged and matured in recent years. In 2022, the LSPosed framework has become the mainstream framework used in software modification. Compared with the XPosed framework, the LSPosed framework is more difficult to detect.

Taking detection points such as feature files as an example, the reasons why the LSPosed framework is relatively difficult to detect are as follows:

In addition, the LSPosed framework has the following advantages:

1. LSPosed was designed to be natively compatible with XPosed, so existing XPosed modules do not need to

Changes can be made to run on the LSPosed framework.

2. For developers, LSPosed still uses the Xposed development kit to develop modules, and there is no additional learning cost.

You can easily develop the desired modules on the LSPosed framework.

3. At present, the maintenance and update of the LSPosed framework are relatively stable, so there is no need to worry about usability issues.

3.3.2 Customized ROM modification has become the most mainstream method of modification at present.

Customized ROM modification: Judging from Threat Hunter's offensive and defensive practice and actual customer testing results, the success rate of software modification is not high. In order to improve the success rate, threat actors are also constantly developing lower-level modification technologies, including custom ROM modification.

Positioning ROM is not a new technology. Its core principle is to modify the Android source code by modifying it. Customized ROM modification technology became more mature in 2022: On the one hand, there are professional groups responsible for maintaining the ROM packages (including drivers) of various brands of mobile phones.

On the other hand, there are professional groups responsible for unlocking the device locks of various brands of mobile phones. With the cooperation of multiple parties and mature operation, there is no need to create a "criminal tool" from scratch. Currently, custom ROM modification has become the most mainstream method of modification.

Compared with software modification, the advantages of custom ROM modification are as follows:

1. The source code modified by the ROM modification does not run in the target application process, so the defender cannot detect it.

head-on confrontation;

2. ROM modification does not require rooting the phone, so defenders cannot mark device risks by detecting the Root environment;

Detection point	Xposed framework	LSPosed framework
Signature files	Xposed modifies the ART virtual machine, leaving signature files such as libxposed_art and the development package XpsedBridge.jar	Not present
Stack inspection	Xposed modifies zygote, leaving the signature stack frame de.robv.android.xposed.XposedBridge.Main	Not present
Active class loading	Xposed adds its own classes to bootclasspath, so classes from the Xposed API can be loaded actively to detect it	Not present

How Xposed and LSPosed differ on common detection points

Source: Threat Hunter original report, page 27. Table re-typeset in English from the original.

3. ROM modification can easily modify any information of the device and has high stability.

Why is it difficult to detect customized ROM modified machines?

If an electrical appliance is compared to the target of modification, and controlling its power supply is compared to the modification process, software modification is like "controlling the power supply into the room", which is easily detected, while ROM modification is like "directly controlling the power plant", which can cause remote destruction from the source, making it difficult for defenders to confront it head-on.

The specific technical principles are as follows:

We take modifying the IMEI value of the device as an example to explain the technical principles of custom ROM modification. On the Android system, the getDeviceID function called to obtain the IMEI value is actually an IPC call. The responder is the system's Phone service (the corresponding process package name is com.android.phone), and will eventually call the Phone.getDeviceID function. By rewriting this function, it is judged based on the uid of the IPC caller whether it is the target application for modification; if so, call getHookValue to return the fake IMEI value; if not, return the real IMEI value. The entire process looks like this:

3.2 In the positioning technology, “hijacking system location services” is commonly used by threat actors.

Changing the positioning refers to modifying the information that the device can use for positioning, including GPS, wifi, base stations, etc., thereby "disguising" the device to a specified address. Location-changing technology is widely used in various business frauds, such as:

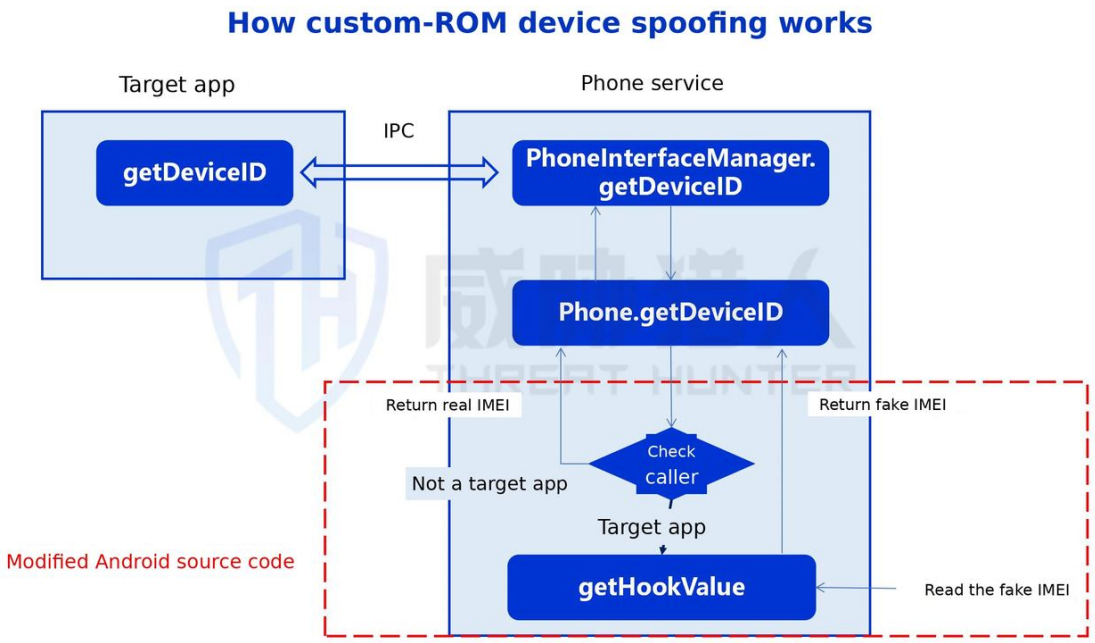
1. Forge false driver travel records to defraud platform subsidies;

2. Change the positioning to a specific location and use the “nearby people” function of social software to attract pornographic traffic;

3. Participate in marketing activities in limited areas, and obtain event qualifications by modifying positioning to break through restrictions.

There are several main ways to change GPS positioning:

1. A relatively basic way is to inject positioning information into the target App through Hook GetLastLocation or



How custom-ROM device spoofing works: the modified Phone service returns a fake IMEI to the target app

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

GetLastKnownLocation function, forges the returned latitude and longitude information. This method is easier to detect, and threat actors are rarely used anymore;

2. GPS information can also be forged through customized ROM technology. The principle is similar to that of modifying the phone. This method has not been hacked yet.

products are commonly used;

3. At present, hijacking system location services is commonly used by threat actors. Hijacking system location services uses Hook key functions and fakes

The return value of the constructor is difficult to detect because it is not in the target application process space.

Hijacking system location services is commonly used by threat actors. Its technical principles and specific steps are as follows:

Principle: In the Android system, obtaining GPS information will call the system's location service; this service runs in the system_server process, and the corresponding Java class is: com.android.server.LocationManagerService. Therefore, by hijacking the relevant functions in LocationManagerService, the effect of forged positioning can be achieved.

Steps:

1. Inject malicious modules into the system_server process;

2. The entry code of the malicious module is called through Class.forName reflection to find the LocationManagerService.

object;

3. Hook multiple functions of the LocationManagerService object, including the getLastLocation function:

4. In the hijacked getLastLocation function, determine whether the location needs to be changed. If so, construct a Location

Object, fill in the fake latitude and longitude information and return; if not, call the original getLastLocation function and return.

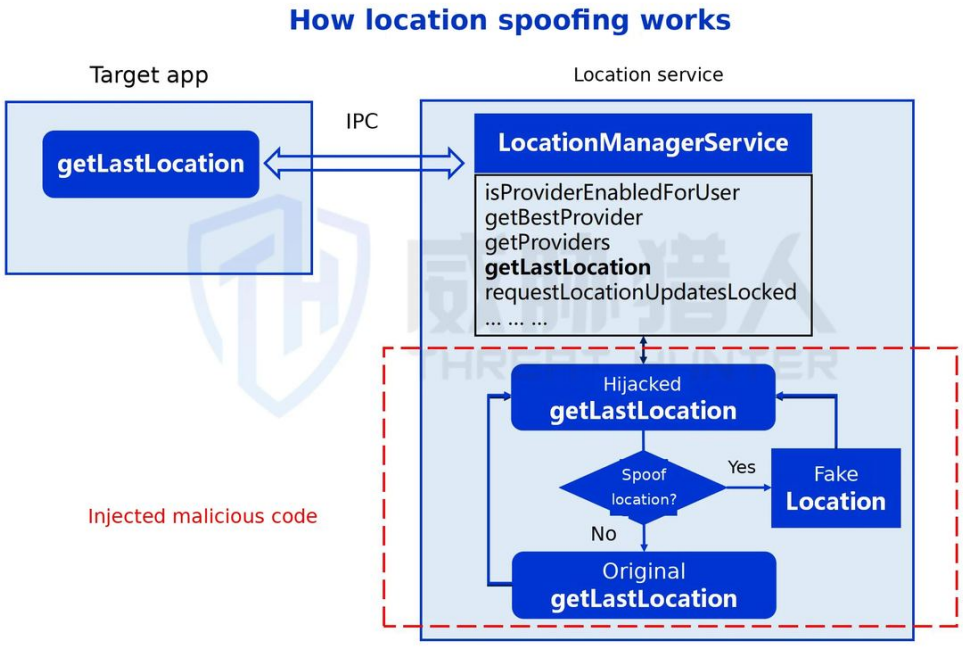
3.3 In face authentication bypass technology, custom ROM hijacking cameras has become a common attack method

Face authentication bypass, threat actors are commonly known as "passing the face" or "passing the face." As more and more applications perform real-name authentication and use face recognition technology, the use of face authentication bypass technology by threat actors becomes more common, including custom ROM hijacking cameras, cloud mobile phone virtual cameras, etc.

Customized ROM hijacking of cameras is also achieved by modifying the Android source code. Since this technique rewrites the lower-level Android source code, it is difficult to detect and has become a commonly used attack method for camera hijacking by threat actors in 2022.

The process of custom ROM hijacking the camera is as follows:

1. When the application uses the camera function, the Camera.open function will be called to open the front or rear camera, and finally



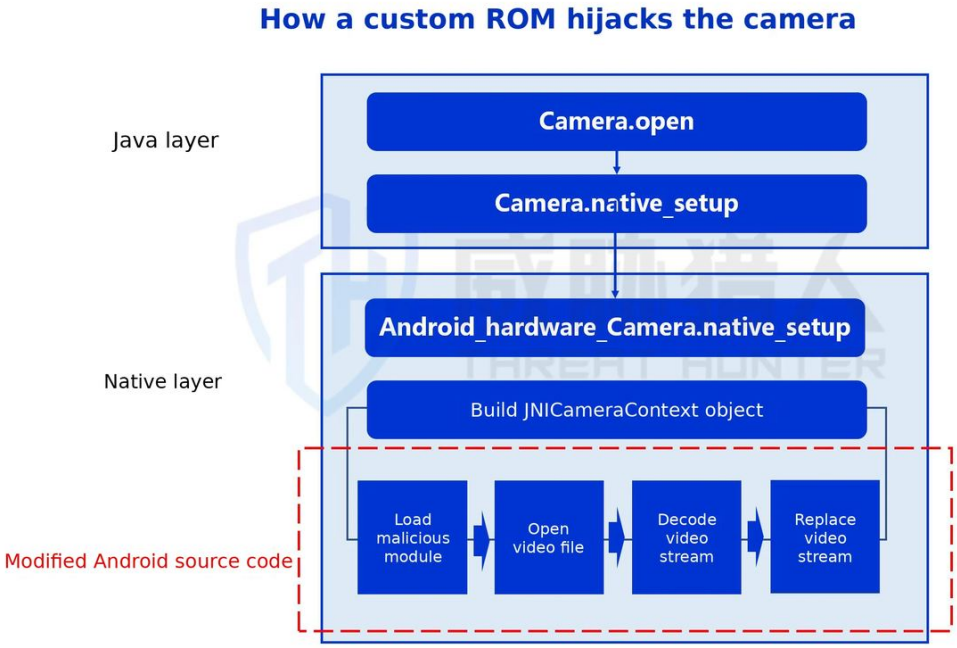
How location spoofing works: injected code hijacks getLastLocation in the system location service

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

Finally, libandroid_runtime.so entering the Native layer calls the android_hardware_camera.native_setup function;

2. The native_setup function will construct a JNICameraContext object (camera context), and operate

Use the camera function for this object;



How a custom ROM hijacks the camera: a malicious module replaces the camera stream with a decoded video file

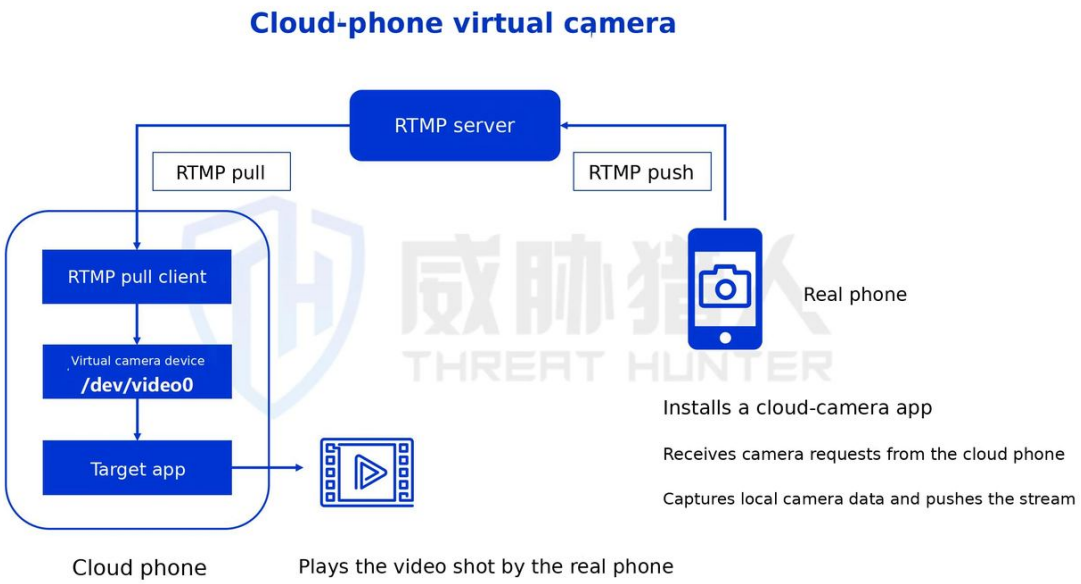
Source: Threat Hunter original report, page 32. Original figure with Chinese text replaced by English.

3. The customized ROM that hijacks the camera rewrites the source code of the JNICameraContext object, and then calls it in its constructor.

A malicious module is automatically loaded;

4. This malicious module integrates the ffmpeg library (an excellent video encoding and decoding library). By calling the ffmpeg library,

Open the video file you want to replace, decode the file, convert it into the video stream format recorded by the camera, and replace it, ultimately achieving the hijacking effect.



Cloud-phone virtual camera: a real phone pushes its camera stream to the cloud phone over RTMP

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

In addition, Threat Hunter discovered through Blue Team's offensive and defensive practice that cloud mobile phone virtual cameras can also bypass face authentication. There are currently many cloud mobile phone platforms on the market, most of which are developed based on Rockchip's RK series chips. Some cloud mobile phone platforms have developed and provided "remote virtual camera" functions. Judging from the actual test results, the cloud mobile phone virtual camera has a higher success rate in bypassing face authentication.

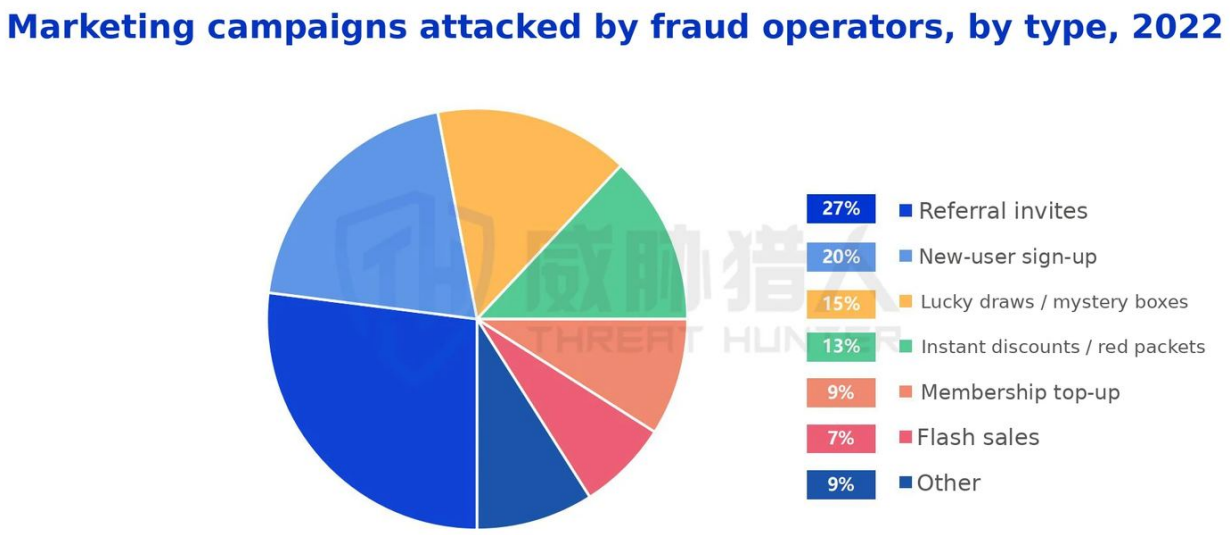
Faced with the increasingly rampant threat actor technologies such as machine modification, positioning modification, and face authentication bypass, it is difficult for enterprises to confront them head-on from a single technical perspective. They can promptly monitor and analyze various threat actor resources using this technology from the intelligence dimension, and carry out targeted defense in a timely manner.

cybercriminal groups attack scenario analysis

4. Analysis of cybercriminal groups attack scenarios in 2022

4.1 Marketing fraud will still be the main attack scenario for cybercrime ecosystem in 2022

When companies carry out marketing activities, they often invest various rewards such as cash, physical or virtual goods to attract users, but they also attract a large number of threat actors to participate in the activities and collect rewards. In 2022, marketing fraud will still be the most important attack scenario for cybercrime ecosystem, with attack targets covering all industries. The following are the more common types of activities in 2022:



Marketing campaigns attacked by fraud operators, by type, 2022

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

In 2022, in order to stimulate consumption in various industries, instant cash discounts have become an important marketing activity type. Among the top-ranked activity types, except for instant cash discounts, other activity types have also ranked high in previous years. Instant discount is a cash coupon issued to users, which can be deducted when customers consume.

In 2022, in order to stimulate consumption in various industries, instant discounts have become an important type of marketing activities. Many banks have launched various forms of immediate discount activities. Due to the lack of marketing fraud prevention and control experience and means, when event participation qualifications and monetization methods are relatively loose and simple, it is extremely vulnerable to cybercriminal attacks.

Take the fraud attack suffered by a bank’s instant bonus event as an example. Users who participated in the event could each receive an instant bonus of 5 yuan. threat actors found a way to monetize the event and launched a large-scale sustained attack. It is estimated that the loss in marketing expenses was nearly 1 million. The entire attack process is as follows:



Instant-discount campaigns run through a mobile payment app

Source: Threat Hunter original report, page 36. Original image retained.

Large-scale attacks launched by professional groups of threat actors cause great losses to enterprises. Such attacks often require the following two elements:

1. A large number of fake accounts: The benefits of promotion abuse on a single account are often not too high, so threat actors generally use a large number of fake accounts to

Use fake accounts to accumulate income. The main source of fake accounts is illicit SIM cards. How to effectively identify illicit SIM cards has become the key to combating marketing fraud;

2. Automated attacks: Automated attack tools developed for marketing activities, which can efficiently complete registration, new recruits, assistance, etc.

There are two main methods of automated attacks to complete event tasks and collect event rewards:

1. Machine modification + group control: Multiple devices are faked through machine modification technology, and multiple devices are controlled in batches through group control technology. For this attack method, how to effectively identify risky equipment environments becomes the key.

How fraud operators attack instant-discount campaigns

Campaign rule	How fraud operators attack it
Each phone number can claim only once	Fraud operators registered large numbers of accounts with illicit SIM cards from code-receiving platforms
Users must complete business verification	By scraping business-lookup and public-disclosure websites, fraud operators stockpiled large amounts of company information, including company names, business licences and the personal details of legal representatives
The CNY 5 instant discount can only be redeemed with a purchase	They join lucky-draw tasks costing CNY 5.16 each but actually pay only CNY 0.16, and the lucky-draw tasks can be traded for cash

How fraud operators attack instant-discount campaigns

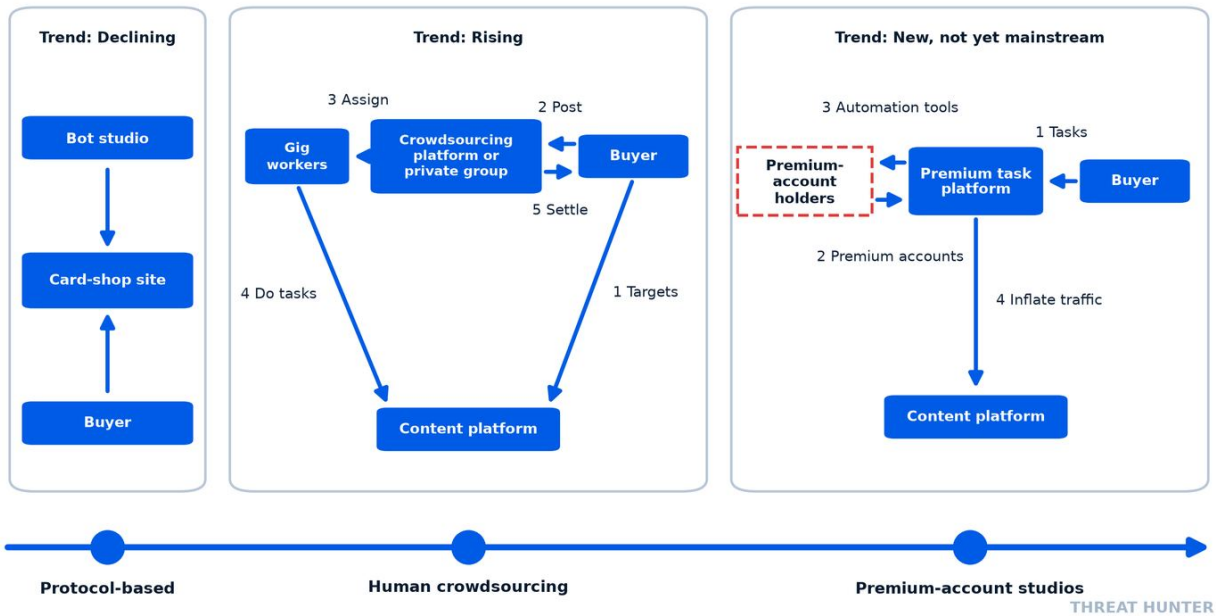
Source: Threat Hunter original report, page 37. Table re-typeset in English from the original.

2 Protocol attack: Crack registration, login and activity-related API interfaces, and batch forge interface requests. For this attack method, the key is to strengthen the security of API interfaces and how to identify risky traffic.

4.2 The traffic manipulation industry chain continues to evolve, and a new type of “premium account” traffic manipulation quietly appears

In today's era of "traffic is king", volume traffic manipulation has become an unspoken "hidden rule" in the Internet industry. Since major content platforms use data such as reading volume, number of fans, and number of likes as criteria for judging influence, content publishers do not hesitate to create false traffic data in order to improve rankings and gain higher exposure.

Traffic-manipulation risk scenarios on content platforms



Traffic-manipulation risk scenarios on content platforms: protocol-based manipulation is declining, human crowdsourcing is rising and premium-account studios are a new, niche model

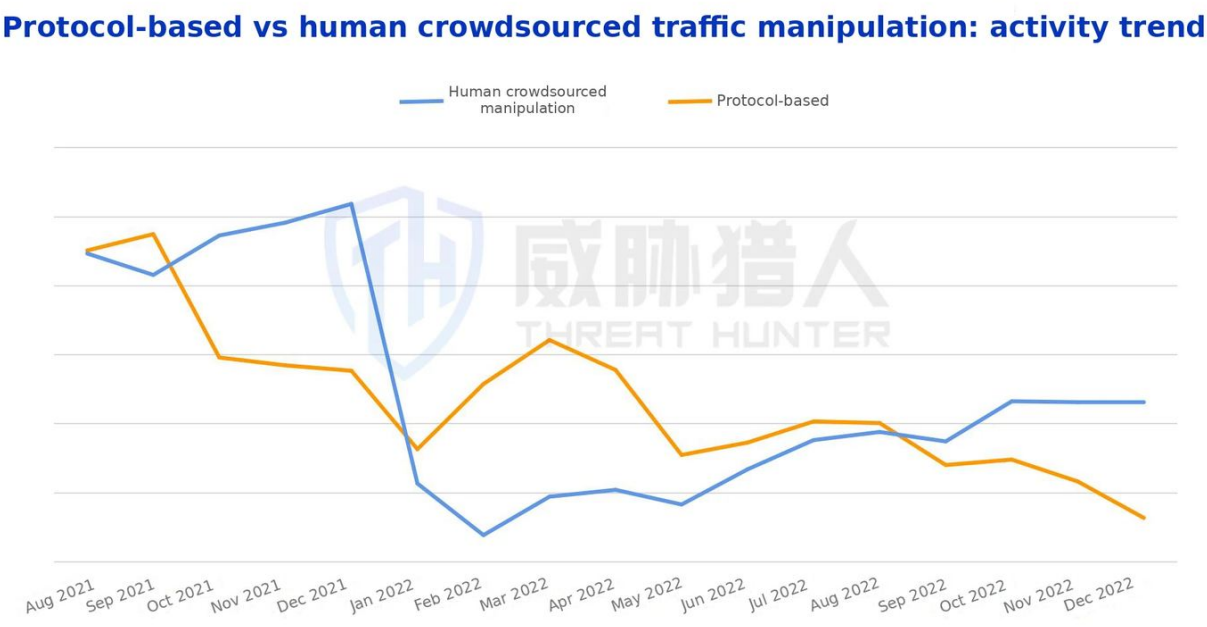
Source: Threat Hunter original report, page 38. Redrawn in English from the original figure.

Under the dominance of traffic thinking, data fraud is prevalent. In 2022, false volume traffic manipulation on content platforms remained popular. In addition to protocol traffic manipulation and human-in-the-loop crowdsourcing, new advanced account traffic manipulation methods have also emerged.

Protocol traffic manipulation: Protocol traffic manipulation is the original means of "traffic fraud", that is, directly using "agent IP + user login status" to simulate the protocol and write code to achieve automated traffic manipulation, which is simple, direct, and low-tech.

human-in-the-loop crowdsourcing traffic manipulation: human-in-the-loop crowdsourcing traffic manipulation refers to brushers posting volume traffic manipulation tasks on the "human-in-the-loop crowdsourcing task platform" or "traffic manipulation task group chat", attracting real users in the form of task bounties, and asking them to manipulate the volume according to a specific process.

The popularity trend of protocol traffic manipulation volume and human-in-the-loop crowdsourcing traffic manipulation volume from August 2021 to December 2022 is as follows. It can be clearly seen that the protocol traffic manipulation volume shows a clear downward trend overall; while the human-in-the-loop crowdsourcing traffic manipulation volume has dropped significantly in early 2022. According to research and analysis, it is mainly affected by the "Qinglang" series of special crackdown activities by the Cyberspace Administration of China, and has shown a gradual recovery and upward trend after February 2022.



Protocol-based vs human crowdsourced traffic manipulation: protocol-based activity fell while human crowdsourcing rose

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

In 2022, the "protocol traffic manipulation volume" dropped significantly, while the "human-in-the-loop crowdsourcing traffic manipulation volume" increased steadily. The main reasons after research and analysis are as follows:

1. The difficulty of protocol volume traffic manipulation increases. With the continuous improvement of the security level of various content platforms, whether it is the difficulty of cracking the protocol

The degree of difficulty, or the difficulty of bypassing machine traffic identification, has greatly increased compared to before, and once discovered, you will face severe punishment from the platform;

2. The effect of human-in-the-loop crowdsourcing far exceeds that of protocol traffic manipulation. human-in-the-loop crowdsourcing of volume traffic manipulation is performed by human participants and is difficult to identify technically.

Threat Hunter cooperates with a domestic leading content platform to conduct human-in-the-loop crowdsourcing traffic manipulation tests. The actual test success rate is very high and the average speed is very fast. The average time to complete the task is only 4 minutes;

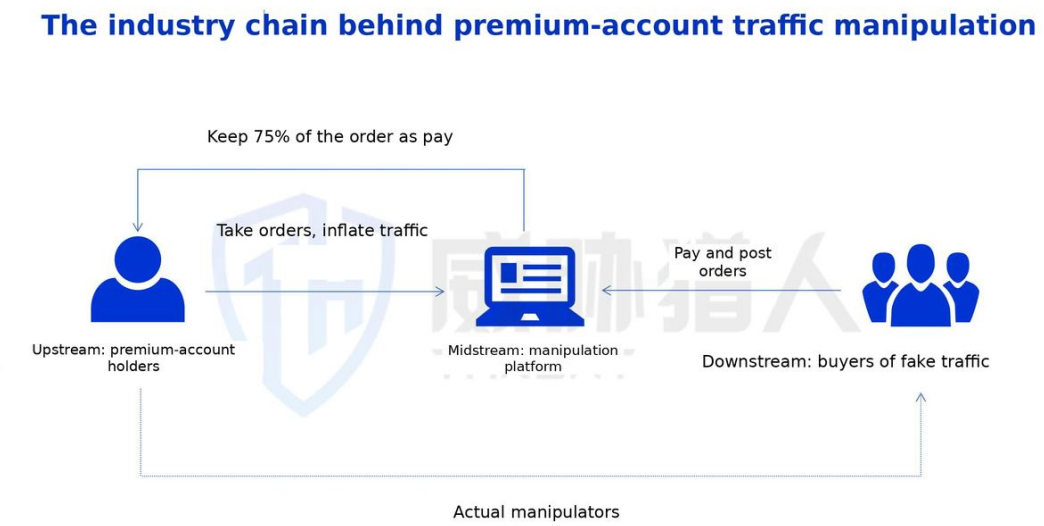
3. human-in-the-loop crowdsourcing tasks are affordable. At present, the main types of tasks for real-life crowdsourcing are: downloading, commenting, likes,

Browse, collect, follow, like, vote, etc. The price of these tasks is not high, the unit price is around 0.2 yuan/item, and buyers can completely accept this price;

4. Special crackdowns will have a greater impact on the traffic manipulation industry chain. The deterrent effect on the wash volume industry chain during the special crackdown activities of regulatory authorities

Obviously, due to the strong market demand for traffic manipulation, many human-in-the-loop crowdsourcing platforms quickly resumed issuing traffic manipulation tasks after the special crackdown, and the number of tasks continued to rise.

In 2022, human-in-the-loop crowdsourcing has become the most important way for threat actors to increase their trading volume. In addition, for top content platforms, threat actors’ volume traffic manipulation has derived a new method of traffic manipulation volume: advanced account traffic manipulation. Its traffic manipulation accounts have the characteristics of high level, rich content, and large number of fans, such as "Thousands of Fans", "Thousands of Fans", "Thousands of Fans and Thousands of Likes", etc. Since such accounts have greater credibility and influence on the platform than ordinary accounts, they have higher weight in terms of ratings, rankings, etc., which can achieve better traffic manipulation effects.



The industry chain behind premium-account traffic manipulation

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

4.3 The effectiveness of automated fraud is getting worse day by day, and human-operated fraud has become the main means of e-commerce fraud.

In the e-commerce scenario in 2022, due to the increasingly perfect platform fraud controls, the effectiveness of automated fraud is getting worse. human-operated fraud has become the main fraud method of the cybercrime ecosystem, and the risks are mainly concentrated in four sub-scenarios: shop fraud, scalpers, full discounts, and malicious compensation.

1. Store traffic manipulation: Store traffic manipulation refers to platform sellers paying to entrust cybercrime ecosystem to manipulate orders, through traffic manipulation tools, human-operated traffic manipulation, etc.

Purchase goods from designated platform sellers and fill in false positive reviews to increase store sales, credibility and ratings, and gain platform traffic.

Store fraud not only misleads consumers' shopping decisions and triggers unfair competition among stores, but also seriously affects the normal operation of the platform.

In 2022, Threat Hunter monitored more than 150,000 fraud reports related to e-commerce platforms, an increase from 2021

26. 15%.

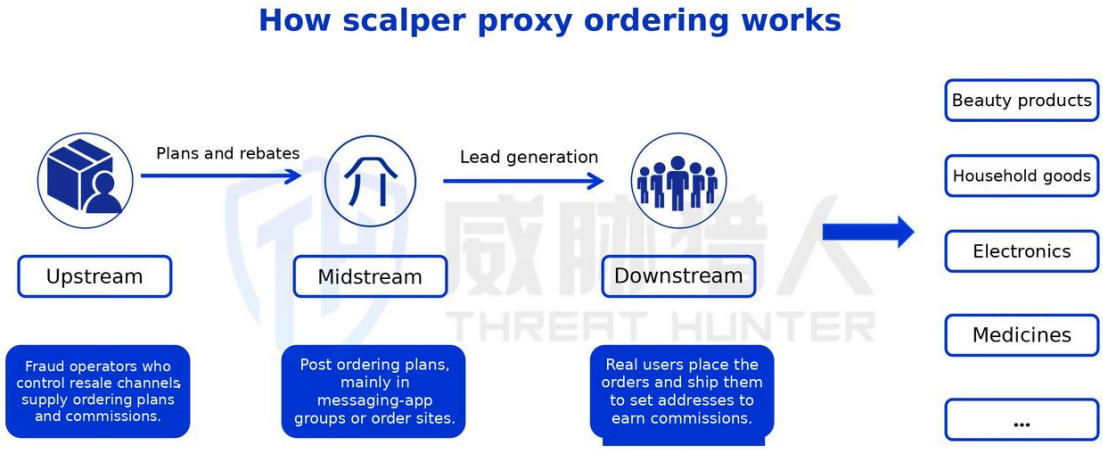
The main methods of fraud in stores in 2022 are as follows:

The technique of traffic manipulation orders is introduced. After accepting the task, real brushers buy goods from designated platform sellers and fill in false positive reviews to increase store sales, credibility and ratings. The live streaming anchors hang low-value welfare products in the product

window of their live broadcast room instead of the merchant's main products. The purchase link points to the fraud merchant. By attracting real users to buy + praise, it improves the overall ranking of the store. The whole process only requires the store to cooperate with scanning the code.

2. Scalper Underground: Scalper Underground refers to the cybercrime ecosystem who hires human participants to place orders remotely to collect discounted products in batches that are limited to purchases during the event.

A mature industrial chain has also been formed. cybercrime ecosystem monitors the discounted products of various merchants in real time, and publishes subscription plans through private chat groups on messaging apps, as well as ordering websites. Real users place orders according to the product links and addresses provided by cybercrime ecosystem, and earn commissions provided by cybercrime ecosystem. cybercrime ecosystem then resells the products at a profit after receiving them.



How scalper proxy ordering works: upstream operators supply plans, midstream posts them and real users place the orders

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

Scalpers have resulted in a large number of preferential products being snatched up by specialized groups of threat actors, while normal users are basically unable to enjoy the discounts, and companies waste a lot of marketing expenses. Over time, normal users will even be lost to the resale channels of threat actors.

The core of the next-generation industry chain is: "Place an order and ship it to a specific address." The drop-shipping product plans released by scalpers through different channels include ordering products and a unified ordering address. Behind the unified address, there are often large receiving groups/large cargo owners who collect products from a large number of scattered drop-shipping groups across the country. Therefore, the platform can collect and analyze such order addresses and implement corresponding fraud-control strategies for such orders/accounts.

3. Get the full discount: Get the full discount means that the promotion-abuse actors studies the full discount requirements of the e-commerce platform to purchase target products at the best price.

Choose another product to combine the order to meet the full discount conditions, and then return the combined order after payment. It may lead to the risk of a large number of goods being returned in a short period of time, as well as merchant data anomalies and inventory pressure.

In 2022, Threat Hunter detected a total of more than 680,000 reports related to "getting full discounts", involving more than 1,000 groups of threat actors, and the overall trend is on the rise. It is worth noting that during major promotions on e-commerce platforms, the risk of "getting the full discount" is particularly common and the consequences are more serious.

Take the platform’s cross-store “collection discounts” during the big promotion period as an example:

During major sales, the platform often supports cross-store discounts. Most of the products can be easily disseminated through passwords and orders can be placed quickly. At the same time, the platform and stores support unconditional refunds. The same product tip for "getting together for a discount" is often generated by different promotion-abuse groups with different passwords and widely spread in social group chats. Therefore, the products that are sold together will face the risk of a large number of returns in a short period of time.

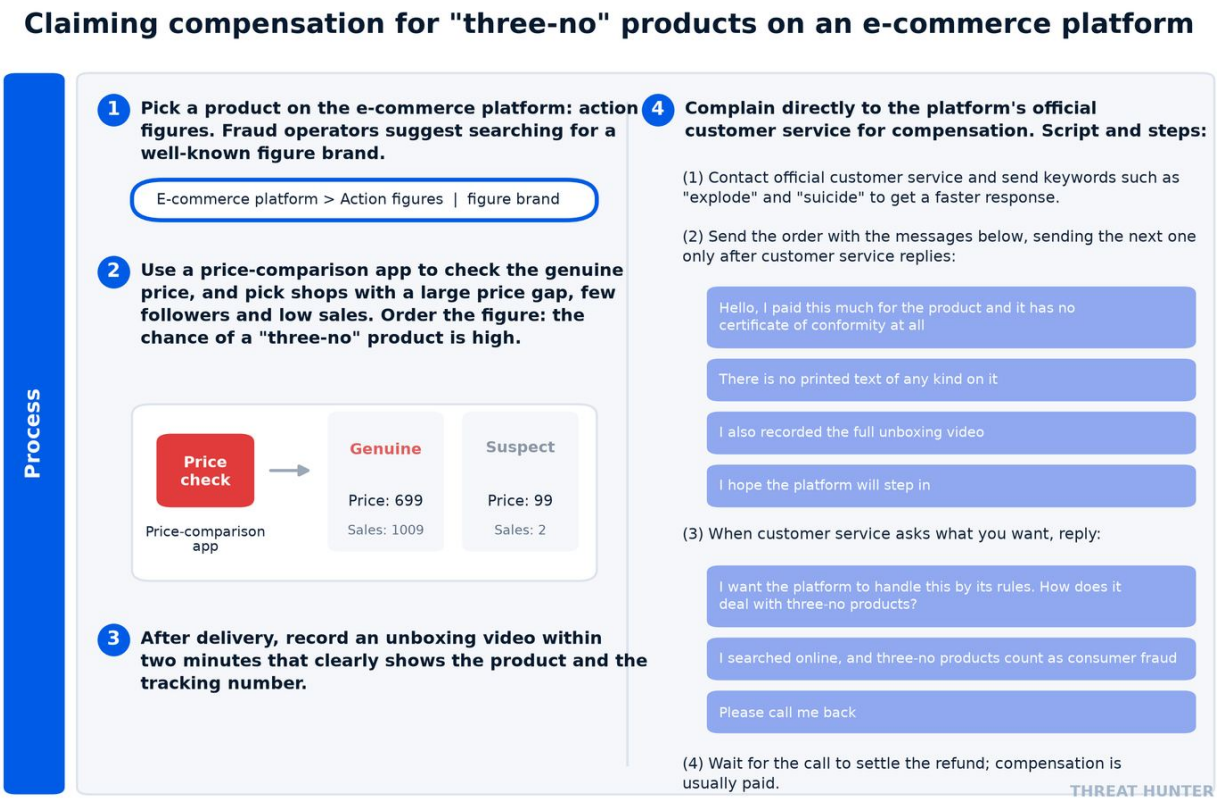
4. Malicious compensation: Malicious compensation refers to cybercrime ecosystem or professional anti-counterfeiters taking advantage of laws, regulations, and e-commerce related prohibition rules to make money through

Merchants place orders for goods and maliciously initiate after-sales applications, putting pressure on merchants and platforms for compensation, by making lies or reporting to relevant departments. Some compensation tutorials have been widely disseminated and implemented through traffic diversion, payment, etc., which has greatly affected the normal operations of merchants and platforms.

In 2022, Threat Hunter discovered more than 30 cases of cybercrime ecosystem malicious compensation schemes by monitoring relevant cybercrime ecosystem forums and communities, mainly concentrated on leading e-commerce platforms. Through further analysis of the plan, it was found that the current compensation plan mainly focuses on issues such as non-delivery, prohibited words in product promotion, counterfeit sales, three noes, contraband, food safety, etc. Find stores with these vulnerabilities and initiate malicious after-sales applications.

Take the "Three No Product Compensation" plan of an e-commerce platform as an example:

The plan shows the compensation ideas and operation process, including how to filter product links for compensation, ordering, key points to note when receiving goods, compensation techniques, etc. The specific content is as follows:



How fraud operators claim compensation for "three-no" products on an e-commerce platform

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

4.4 Financial credit fraud brings large economic losses to financial institutions

With the development of finance + Internet, while the financial industry provides users with flexible and convenient services through digital transformation, it also faces various fraud threats from threat actors that continue to iterate and evolve. Among them, financial credit fraud is the most serious, causing bad debts and large economic losses to financial institutions.

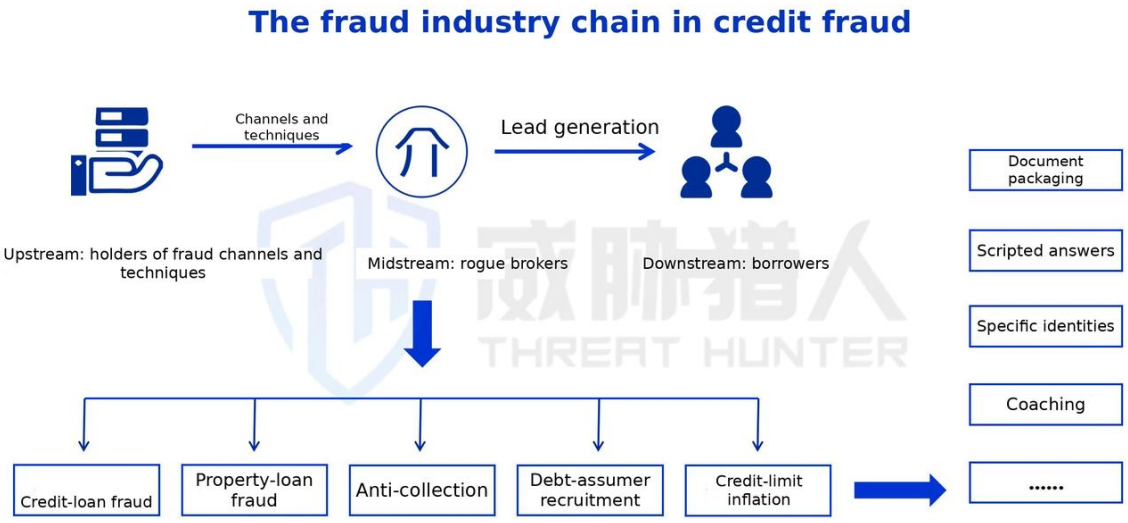
Financial credit fraud: threat actors use loopholes in loan approval to apply for loans for borrowers, or use specific words and other methods to successfully apply for extensions and interest exemptions for borrowers, and the intermediary earns high commissions from this. This type of malicious behavior can cause credit institutions to lose funds and large amounts of bad debts.

The current industrial chain structure of threat actors in credit fraud scenarios is as follows:

- Upstream are mainly those who master fraud channels or technologies and are responsible for providing loan channels and technologies;
- The midstream is mainly the credit intermediary group, responsible for the dissemination of fraud plans and actual agency operations
- The downstream is mainly the loan fraud group. As the actual lenders, the loan fraud groups are mainly divided into several categories:

1 Users who were rejected by banks due to lack of qualifications;

2. Users who want to perform operations such as interest refunds and refunds;



The fraud industry chain in credit fraud: upstream channel and technique holders, midstream rogue brokers and downstream borrowers

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

3 Users who were instigated by intermediaries or maliciously concealed to take out loans.

In credit fraud, the attack scenarios of threat actors can be subdivided into: loan fraud, anti-collection, debt recruitment, Xintong card limit increase, interest refund and fee refund, etc. The ultimate goal is to achieve the purpose of identity verification by forging qualification certificates. The main fraud ideas include but are not limited to forging qualifications and bank statements, using specific words to counter collection, etc.

The specific malicious activity ideas of credit fraud are as follows:

- 1 Forging loan user qualifications: threat actors help defaulting users get loans by forging information. The essence is to falsify applicant information. Common falsified items include: workplace, real estate information, provident fund, salary flow, etc.

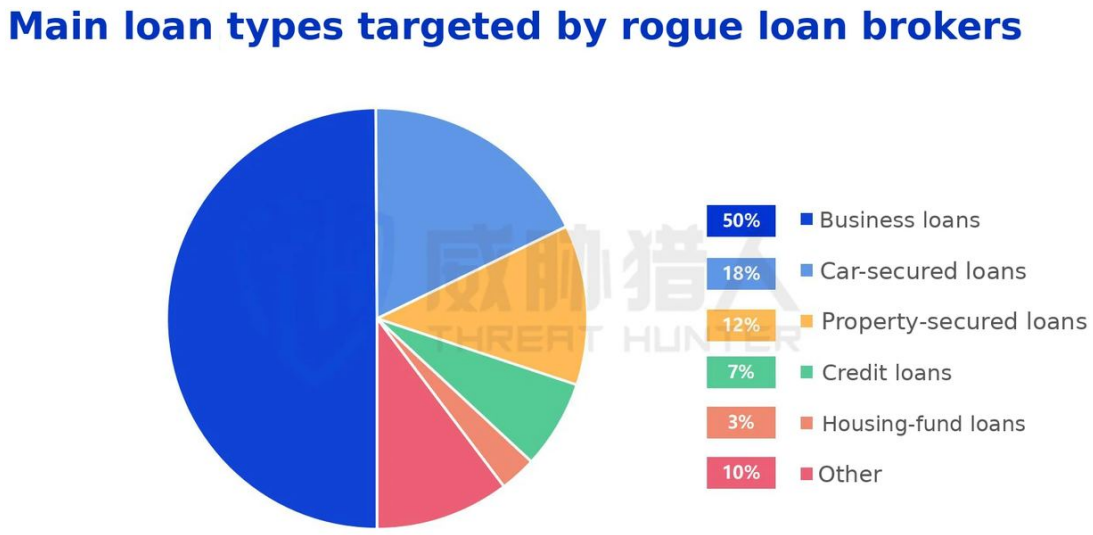
2. Counterfeiting bank apps to produce bank statements: threat actors create false statements by counterfeiting bank apps, making it difficult to detect abnormalities.

This method mainly takes advantage of the information gap between different banks: assuming that threat actors want to apply for a loan at Bank A, and create a fake app and fake statements for Bank B. During the application process, threat actors will show Bank B's fake app and statements to the staff of Bank A, so it is difficult for Bank A to find abnormalities without careful identification.

3. Provide specific anti-collection techniques: In 2022, a large number of credit customers had credit overdue due to the epidemic. Many threat actors provide anti-collection services to these customers. The most important method is to provide specific anti-collection techniques and specific methods. Services include suspension of debts, penalty interest reduction, complaint compensation, credit repair, etc.

Among the main loan types attacked by black intermediaries, enterprise loans accounted for nearly 50%. In 2022, Threat Hunter detected that the main loan types attacked by black intermediaries include enterprise loans, car mortgage loans, housing mortgage loans, credit loans, provident fund loans, social security loans, insurance policy loans, entrepreneurial loans, decoration loans, tax loans, current loans, tobacco loans, consumer loans, academic loans, etc. Among them, enterprise loans have become the primary target of financial credit fraudsters, accounting for nearly 50%.

4.5 Multiple money laundering incidents were captured in 2022, with the amount involved estimated to be over 100 million



Main loan types targeted by rogue loan brokers: business loans account for nearly half

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

The method of money laundering through recharge and payment apps is used by many threat actors. In 2022, the Threat Hunter risk intelligence platform captured multiple related cases, involving more than 10 apps, and the amount involved is estimated to be over 100 million.

Taking a captured phone charge money laundering incident as an example, the threat actors' crime process is as follows:

1. Gamblers recharge on illegal websites such as online gambling and pornography, and choose the payment method to recharge phone bills;

2. When gamblers click to recharge, they will jump to an illegal aggregated payment platform;

3. At the same time, ordinary users purchase discounted/low-price phone bills through some channels and recharge their phone bills;

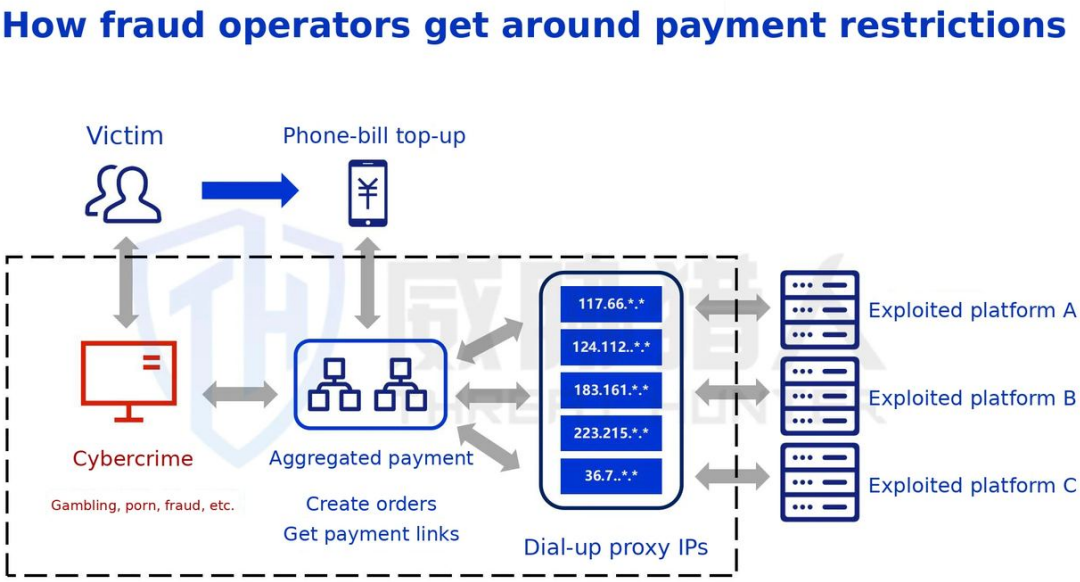
4. The aggregated payment platform initiates equal phone recharge requests on certain apps based on the recharge amount, generates orders and obtains

Payment link;

5. The aggregation payment platform returns the obtained payment link to the gambling platform;

6. The gambler completes the phone bill recharge according to the payment link and successfully "raises points".

As a result, the phone bills of ordinary users turned into gambling funds for gamblers.



How fraud operators get around payment restrictions: gambling funds are paid through phone-bill top-ups on exploited platforms

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

Threat Hunter intelligence personnel discovered that illegal fourth-party platforms provide comprehensive payment and settlement services to gambling platforms by aggregating interfaces with third-party payment platforms, cooperative banks and other service providers. On this basis, the Sifang Payment Platform needs to generate a large number of recharge orders, which are easily recognized as abnormal behavior by the recharge service platform. In order to avoid the detection and supervision of the recharge service platform, the illegal Sifang Payment Platform often uses "agent IP" to hide its identity, making the illegal activities of online gambling platform payments more concealed.

Risk combat ideas

5. Risk confrontation ideas

cybercriminal groups are becoming increasingly rampant, causing serious harm to various industries such as the Internet, finance, e-commerce, and games. For the defender, it cannot just be a passive defense, but also requires continuous monitoring and response, and proactively grasp the trends of the cybercrime ecosystem. Therefore, intelligence capabilities become particularly important.

Whether it is a traditional cybercriminal groups attack scenario or the recent increasingly serious data security issues caused by improper API management and control, intelligence can be relied upon to establish a security baseline for risk management.

Leveraging rich cybercrime ecosystem intelligence data, companies can:

In the external cybercrime ecosystem governance, we monitor and perceive attack risks in a timely manner through multiple channels across the entire network, and analyze and extract attack information such as cybercriminal groups' specific trends and tools/materials used, so as to carry out targeted defenses in a timely manner.

cybercriminal groups will inevitably use some resources when launching attacks, such as IP, threat actors' malicious tools, etc. Threat Hunter's rich cybercrime ecosystem intelligence data is used to extract threat actors attack patterns and resource characteristics, match them with abnormal traffic in enterprise business, and quickly identify risks:

1. Use the risk IP tags detected by the Threat Hunter risk intelligence platform to mark customer business traffic. On the one hand,

Continuously monitor changes in risk IP access trends of each business API. On the other hand, by comparing data, analyze the difference between the request behavior sequences of normal users and risk IP under the API, and determine whether the API is at risk of being attacked;

2. For attack IPs, provide label information such as risk IP portrait access times, regions, risks, etc., through API interfaces

Output attack characteristics IOC in real time, and then link with other security systems of the enterprise to block attack traffic in a timely manner to improve blocking efficiency and achieve multi-point defense.

With the help of "intelligence" capabilities, enterprises can comprehensively and timely perceive internal API asset risks and the trajectory and trends of cybercriminal groups from a global perspective, accurately warn and output the attacker's IOC intelligence, etc., and then link the fraud-control system or WAF to quickly deal with attack risks, and face the increasingly severe cybercrime ecosystem risks and challenges, so as to calmly respond and effectively counterattack.