THREAT HUNTER RESEARCH

2020 Cybercrime Ecosystem: Annual Offense and Defense Report

An annual review of cybercriminal capabilities and the intelligence, controls and operating practices used to counter them.

Original publication: 2020-12-25
Research team: Threat Hunter Research Team
Source report: 117 pages

Original report text

> This text version is reconstructed based on the 117-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.

Abstract Entering the 21st century, the popularity of smartphones has begun to gradually attract media and markets that once existed on PCs to mobile terminals. Soon, the business scenarios carried by the Internet showed explosive growth due to mobile attributes, and the ability and willingness of individuals to pay in business models were also rapidly increasing. More and more people are willing to enjoy the services brought by content payment, such as opening VIP memberships, purchasing online courses, etc. At this time, the connection generated by the Internet is no longer just the connection between content and devices, but the connection between scenarios and individuals.

The core resources of the Internet have also changed from devices to individuals. Every netizen who exists on the Internet is the object of competition in the new Internet era. At the same time, cybercriminal groups are gradually shifting to the mobile Internet scenario.

Based on this understanding, Threat Hunter has been accumulating cybercriminal groups attack and defense on the mobile Internet for a long time. Recently, we summarized and analyzed the case accumulation in 2020 and compiled it into this report. We hope that these experience sharing can provide forward-looking reference for enterprises, institutions and practitioners in the construction of future Internet business security, and help enterprises lay a solid foundation for business security.

The main contents of this report are as follows:

In the first part, we will focus on the core risk scenarios of the enterprise, introduce the importance and value of business security intelligence in enterprise security, and demonstrate the corresponding solutions of Threat Hunter;

In the second part, we will introduce the macro- and micro-level evolution trends of the cybercrime ecosystem chain, and conduct case analysis from the dimensions of attack methods, attack channels, and crowd portraits;

The third and fourth parts mainly share the iterations of offensive and defensive technologies, threat-actor tools and cases, and give corresponding offensive and defensive suggestions.

1. Threat Hunter business security intelligence capabilities

Threat Hunter's three major product service lines are based on business security intelligence:

1. Business security intelligence platform

The business security intelligence platform helps enterprises monitor, warn and discover unknown risks. The business security intelligence platform focuses on the core risk scenarios of the enterprise: account security, marketing activities, private messages/dynamic malicious traffic, volume fraud, human-in-the-loop crowdsourcing and other business issues. Analyze the industrial chain structure and gang characteristics of threat actors in each risk scenario, as well as the

channels and methods for threat actors at all levels to deliver messages, threat actors materials, and threat-actor services. Finally, the network threat actors are divided into three groups: resources, services, and monetization according to the supply structure of the industry chain. They conduct intelligence channel mining and monitoring for the cybercrime ecosystem at different stages.



Threat Hunter’s business security intelligence platform

Source: Threat Hunter original report, page 4. Original figure with Chinese text replaced by English.

	Threat-actor need	Solution or supporting industry
Resources	Illicit SIM cards	SIM-card dealers: bulk card activation through virtual carriers and other channels
	Proxy IPs not on blacklists	Proxy IP platforms: pooled dynamic IPs from home broadband and cell towers
	Device information	Device-spoofing tools and IMEI allowlists: fake device fingerprints, purchased allowlists
	Identity data	Data brokers: obtained through database dumps, fraud and trojans
	Company credential documents	Data brokers: resold or forged company credentials
Services	Sending and receiving verification codes	Code-receiving platforms: connect to SIM dealers and receive or send SMS codes on request
	Passing human-verification checks	CAPTCHA-solving platforms: pass checks with AI or human solvers
	Batch attacks	Group-control devices: run actions on many devices at once
	Trading platforms	Account-sales platforms and the dark web: semi-open or hidden marketplaces
	Company credential documents (as labelled in the original)	Money-laundering industry: online shops, crowdsourcing and other laundering services
Monetisation	Online fraud, malicious traffic diversion, promotion abuse, traffic inflation, account theft and laundering, ad-network fraud, email trojans, silent trojans, ransomware, fake orders, online lotteries, blockchain fraud, game cheats, sex-related fraud, online gambling	

Threat-actor needs and the industries that serve them

Source: Threat Hunter original report, page 5. Table re-typeset in English from the original.

Build a risk intelligence platform with panoramic coverage of business scenarios and threat actors attack links, and empower enterprise business security through four major intelligence sections: threat actors tip monitoring, threat actors tool monitoring, threat actors cost monitoring and data asset security.

Layer	Components
Lightweight deployment	Business risk intelligence platform delivered as SaaS; intelligence API output
Rapid alerting and response	Instant risk alerts; daily briefs; weekly reports summarising risk; flexible delivery by email or messaging app; real-time risk awareness
In-depth analysis	Threat-actor post classification, high-value intelligence extraction, threat-actor group profiles, NLP extraction of trending topics | Material cost monitoring, group profiles, code-receiving scenario and regional monitoring, industry material cost monitoring | Tool activity monitoring, attack path reconstruction, key code extraction, threat scenario classification | Risk alerts, data verification, leak source tracing | Login, registration and platform traffic-inflation monitoring
Multi-source data collection	Threat-actor communities: messaging-app groups, forums, dark-web forums, human crowdsourcing platforms | Material platforms: code-receiving and account-sales platforms | Threat-actor tools: macro-scripting tools, autojs, protocol tools, general helpers, app cloners, Xposed plug-ins, proxy IP clients, location spoofers | Data-leak channels: dark-web forums, online documents, code-hosting sites, e-commerce platforms, threat-actor chat groups, second-hand trading, cloud drives | Malicious traffic: honeypot traffic, idle-device traffic inflation
Threat-actor research	Methods, tools, costs, attack chains, organisation and development trends of threat actors

Architecture of the business security intelligence platform

Source: Threat Hunter original report, page 5. Table re-typeset in English from the original.

2. fraud controls basic data labels

It helps enterprises establish a risk intelligence database for the three basic resources of cybercrime ecosystem. The risk identification accuracy is as high as 99.5%, which can be directly used for business judgment; the risk recall rate is as high as 60%, which greatly helps customers reduce risks and losses.

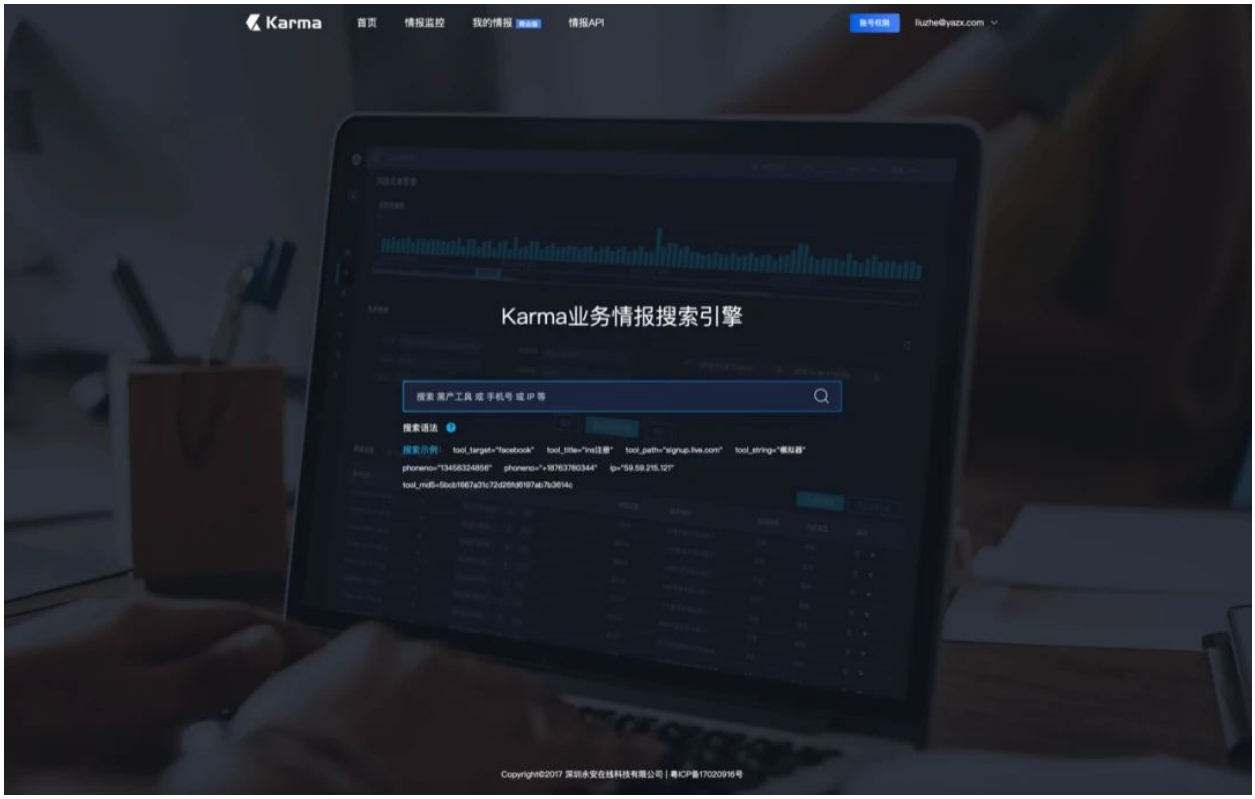
1) Risk phone number identification - identify whether the phone number is a fake phone number held by cybercriminal groups or a real number hijacked by threat actors 2) Dynamic risk IP identification - real-time identification of dynamic risk IPs such as proxy, second dial, mixed dial, proxy second dial, etc. 3) Risk equipment environment - identify more than 30 risk equipment environments such as group control, cloud control, box control, cloud phone, simulator, multiple clones, Root jailbreak, device debugging, virtual positioning, hang-up behavior, etc.

3. Business security services

Helping enterprises apply and monitor implementation intelligence 1) cybercrime ecosystem research service 2) cybercrime ecosystem tool analysis 3) business security Blue Team

4. Karma Business Intelligence Search Engine

The industry's first business intelligence search engine launched by Threat Hunter (register to use: Karma.yazx.com)



The Karma business intelligence search engine

Source: Threat Hunter original report, page 6. Original image retained.

Regarding this business intelligence search engine, we will always provide value to customers around three major capabilities -

Business intelligence investigation and analysis capabilities: You can discover and analyze the latest the cybercrime ecosystem tools, query phone number risk profiles, IP risk profiles, etc.

through the Karma business intelligence search engine. In the future, Karma will also focus on search, connect more risk scenarios and intelligence data, and use AI machine learning to provide more in-depth analysis capabilities to continue to help customers improve query coverage and analysis efficiency.

Business risk perception capabilities: Karma now provides some basic intelligence warning capabilities, such as discovering tools for threat actors that attack your business, monitoring data transactions on the dark web, and price fluctuations of threat actors' liquidation transactions, etc. On the one hand, we will continue to expand the scenarios that early warnings can cover. On the other hand, we will provide more risk perception capabilities in the future. Many of the functions in the iteration may be the first in the industry, so stay tuned.

Business intelligence data API capabilities: API as an extension of the product, including phone number portrait API, IP portrait API, and intelligence monitoring API. Mobile phone number profiling and IP profiling can provide customers with identification/interception capabilities after Karma discovers risks; and the intelligence monitoring API can facilitate customers who build their own intelligence analysis systems to flexibly access external capabilities.

2. The evolution trend of cybercriminal attacks

1. Business model changes bring about changes in cybercriminal groups' core resources

The industrial chain of cybercriminal groups have been following the development of the domestic Internet for more than 20 years. In the early years, cybercriminal groups began to control personal computers as broilers to perform Ddos, flash ads, install rogue software, etc. for monetization. Actual physical computers are the core resources of cybercrime ecosystem. Whoever controls more will make more money.

The reason why the Internet cybercrime ecosystem in this era has this logic is also because the early business model of the Internet was very focused on online advertising. In the PC Internet era, the settlement logic of online advertising was based on computer equipment. Each Internet company also built its own core business logic based on the number of installations, activations, and activity.

At that time, the number of devices was not only the core resource of the cybercrime ecosystem of the Internet at that time, but also the core resource of the entire Internet at that time.

Entering the 21st century, the popularity of smartphones has begun to gradually attract media and markets that once existed on PCs to the mobile terminal. Soon, the business scenarios carried by the Internet showed explosive growth due to mobile attributes, and the ability and willingness of individuals to pay in business models were also rapidly increasing. More and more people are willing to enjoy the services brought by content payment, such as opening VIP memberships, purchasing online courses, etc. At this time, the connection generated by the Internet is no longer just the connection between content and devices, but the connection between scenarios and individuals.

The core resources of the Internet have also changed from devices to individuals. Every netizen who exists on the Internet is the object of competition in the new Internet era. At the same time, cybercriminal groups are gradually shifting to the mobile Internet scenario.

2. The production and circulation of fake accounts are increasing in scale

Based on the changes in the core resources of the Internet, we have observed that the cybercrime ecosystem of the Internet has changed from the previous model of delivering Trojans to users' computers through pornographic traffic and gaining control of the computers and then monetizing them, to a method of registering malicious accounts in various Internet core business scenarios through a large number of phone numbers, and monetizing these accounts in business scenarios.

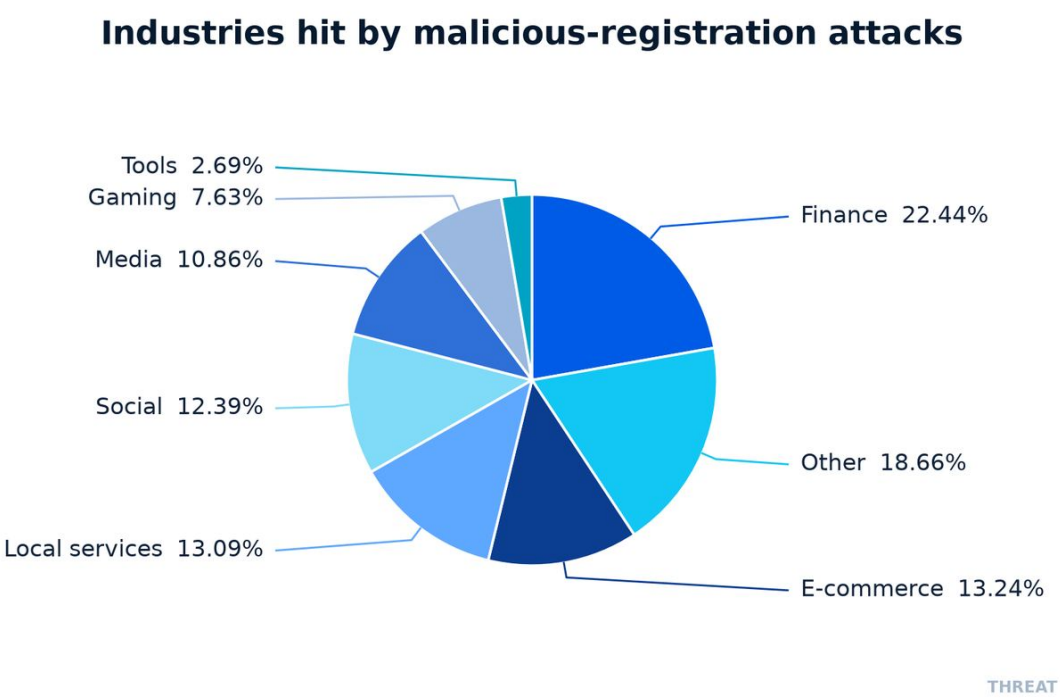
Malicious registration is the starting point of business risks and the core key point of enterprise fraud controls. Today, various attack resources represented by threat actors, represented by malicious registration, have become highly modularized and market-oriented. Gangs at different levels of the industry chain focus on different tasks and cooperate closely. The fundamental reason is that strong automation makes attacks replicable, thereby forming a routine profit model and posing a threat to corporate assets. If an enterprise cannot discover problems in time and adopt effective countermeasures, it will face huge losses in business.

2.1 cybercrime ecosystem malicious activity scenario with malicious registration as the core resource

With the changes in business models, various cybercriminal attacks with fake accounts as the core resources have begun to emerge, such as e-commerce platform profiteering, live streaming platform traffic manipulation, social platform traffic manipulation, and online fraud.

Take the live streaming platform as an example. manipulating traffic volumes can help the anchor to get on various rankings; buying zombie fans for the anchor can increase the number of fans of the anchor; purchasing trolls in the anchor's live broadcast room can increase the popularity of the live broadcast room, etc. On the one hand, these data can be directly converted into cash rewards on the platform, thus making a profit; on the other hand, fake popularity can attract more fans, and then make profits through fan rewards.

According to statistics from Threat Hunter Guigu Lab, attacks launched by malicious registrations across the entire network can reach 8,327,380 times a day. The illicit SIM-card resources involved behind this have an average daily active volume of 1,389,107, and each illicit SIM card carries out an average of 6 attacks per day. Among them, the industries most affected by malicious registration include finance, e-commerce, media, social networking and life services. It can be clearly found that the targets of malicious registration attacks are generally highly profitable or high-traffic. It can be seen that the downstream monetization needs are the fundamental driver of malicious registration.



Industries hit by malicious-registration attacks

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

The picture shows: The proportion of industries affected by malicious registration attacks. The reuse rate of each illicit SIM card is very high, because cybercriminal attacks have obvious liquidity under China's national conditions, that is, the same industry often faces common cybercriminal attacks, and enterprise products with lower attack thresholds and weak protection are more likely to attract attacks.

When the difficulty of attacking a certain company increases, relevant personnel will quickly turn to other companies of the same category. There are certain similarities in the ideas and measures of major enterprises in solving problems, which also results in the high replicability of threat actors' bypass methods and attack tools.

Under such circumstances, if an enterprise does not understand cybercriminal groups attack methods and cannot identify the large number of fake accounts it has, it cannot develop a defense strategy with the lowest cost and least damage to normal business based on the enterprise's own situation.

2.2 Behind the scale of malicious registration is the development of efficiency platforms

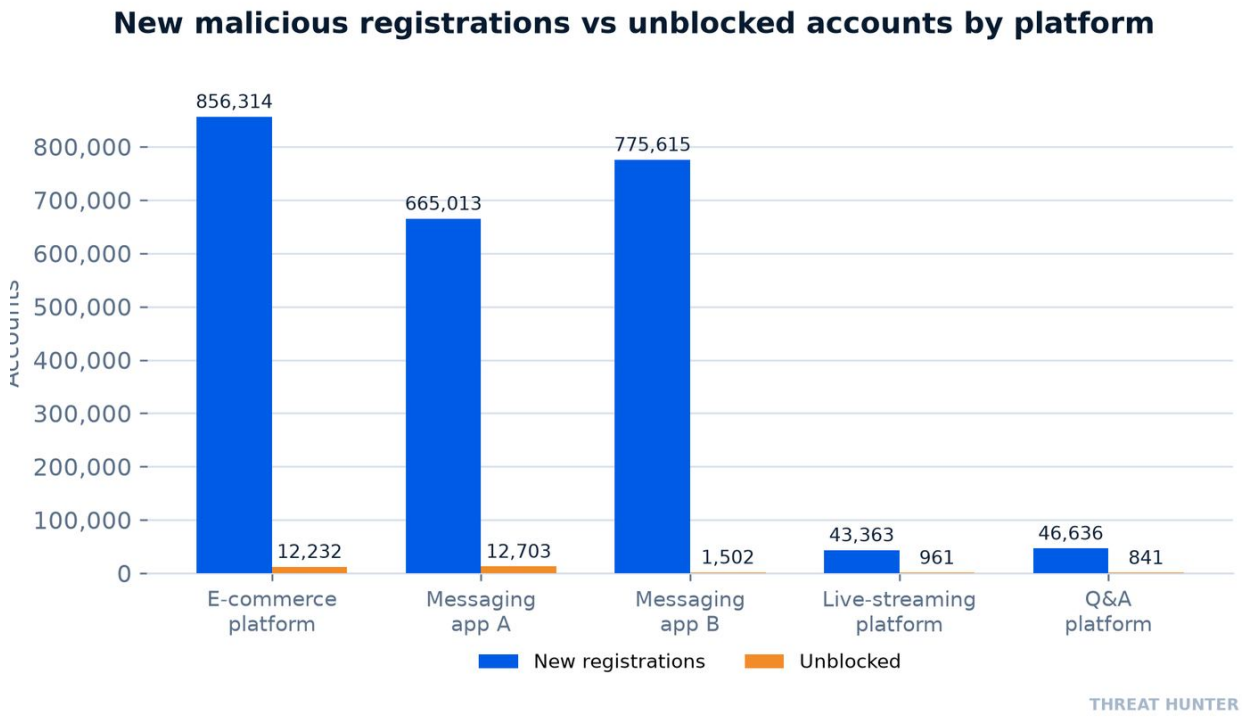
Nowadays, various attack resources represented by threat actors, represented by malicious accounts, have become highly modularized and market-oriented. Gangs at different levels of the industrial chain focus on different tasks and cooperate closely. Ultimately, it is strong automation that makes attacks replicable, thereby forming a routine profit model, posing a threat to corporate assets.

According to the research and analysis of Threat Hunter Guigu Lab, it was found that accounts obtained by malicious registration are consumable commodities. While companies deal with malicious accounts through various security strategies, new maliciously registered accounts will

continue to fill in the missing parts of the malicious accounts. Although some accounts can be unblocked after being blocked by sending text messages, receiving voice verification codes, etc., the actual unblocking rate is extremely low for two reasons:

- First, the time it takes for threat actors to unblock an account is much longer than the time it takes to register an account;
- Second, in many scenarios, cybercriminal groups have completed monetization before the account is banned. At this time, the price and cost of unblocking a banned account is much higher than registering a new account.

The figure below shows the proportion of new maliciously registered accounts and secondary unblocked accounts during the same period:

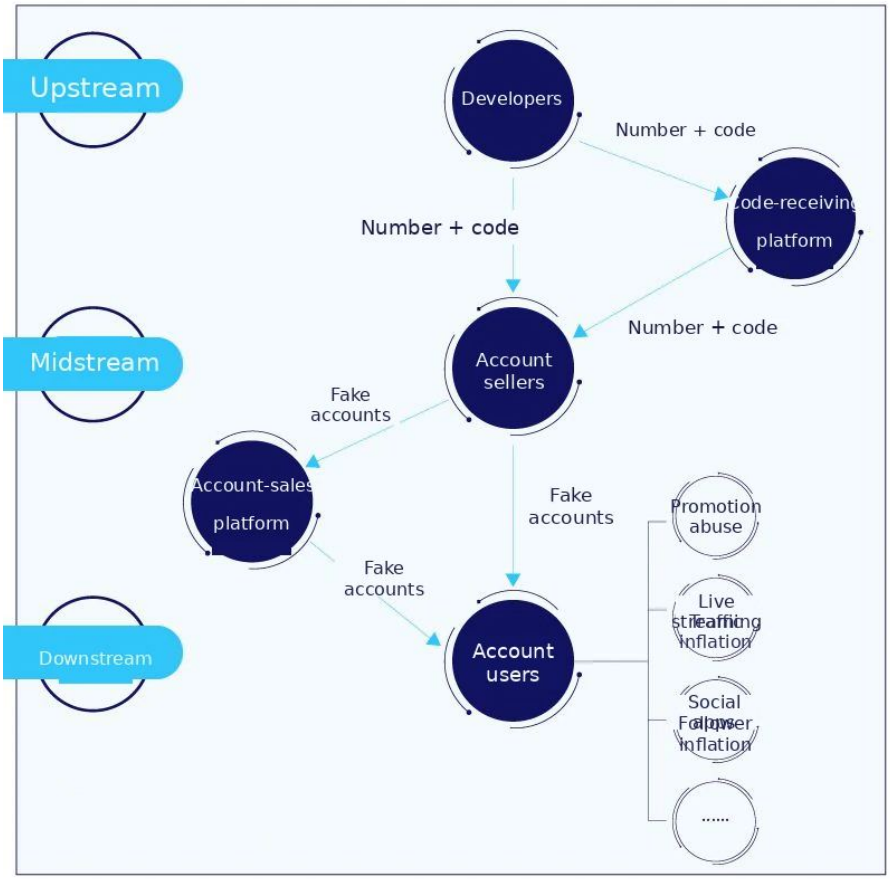


New malicious registrations far outnumber unblocked accounts on every platform

Source: Threat Hunter original report, page 10. Redrawn in English from the original figure.

The picture shows: Comparing the number of new maliciously registered accounts and the number of unblocked accounts, it can be seen that during the same period, the number of new registered malicious accounts was far greater than the number of unblocked accounts. Therefore, in the entire process of large-scale malicious registration, how to improve the efficiency of the entire operation process and reduce the cost of malicious registration is the core key point of conducting malicious activity.

Therefore, in the entire development process of cybercrime ecosystem, "SMS verification-code receiving service", "card issuing platform" and related industries have become a crucial link in the malicious registration industry chain.



How code-receiving and account-sales platforms link the malicious-registration chain

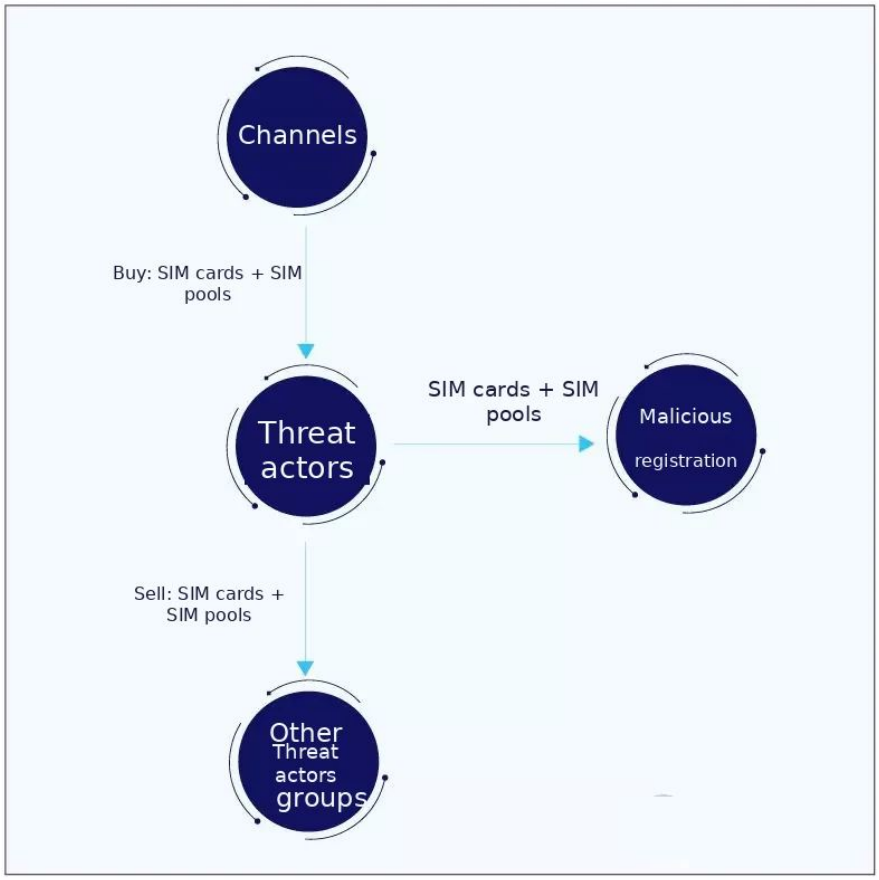
Source: Threat Hunter original report, page 11. Original figure with Chinese text replaced by English.

Pictured: Industrial chain assistance completed using SMS verification-code receiving service and card issuance platform

2.2.1 CAPTCHA-solving service - improve the efficiency of cybercrime ecosystem false registration

The SMS verification-code receiving service is actually a platform for receiving SMS verification codes. It was born in the early days of the mobile Internet. At that time, cybercrime ecosystem purchased SIM pool equipment and inserted hundreds of mobile phone cards to simulate hundreds of natural persons to complete malicious registration of business scenarios. After malicious registration, the equipment and phone cards are resold or rented to another cybercrime ecosystem team for malicious registration in different business scenarios.

This process is actually very inefficient. Because a cybercrime group is responsible for three links:



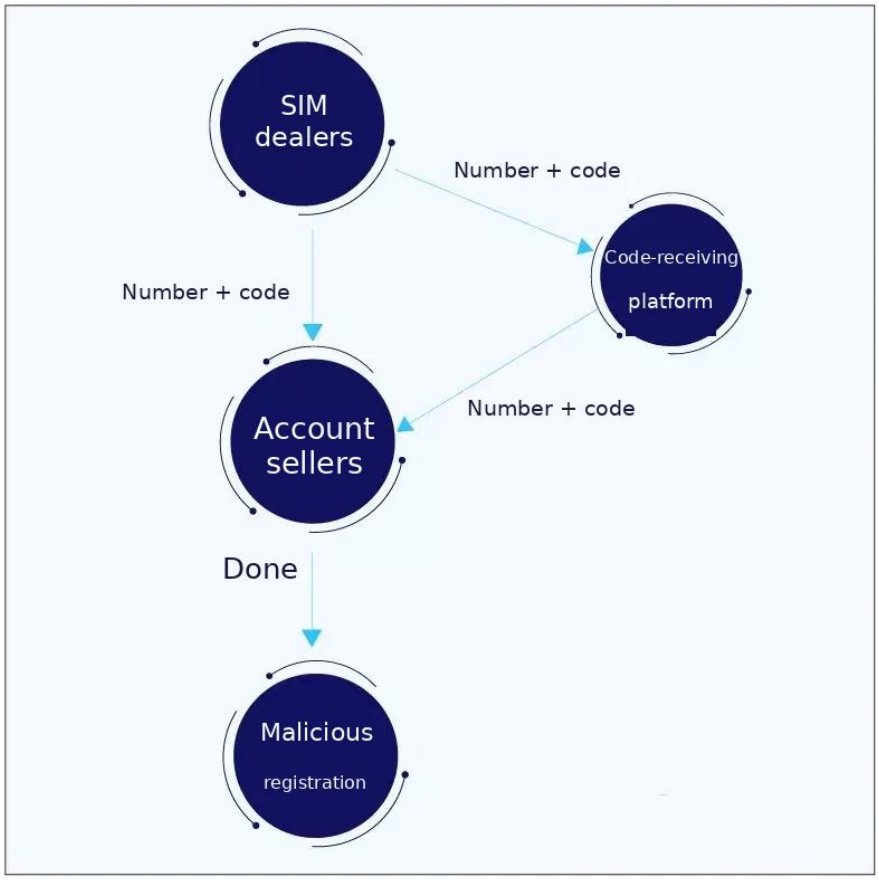
Malicious registration in the past: threat actors ran their own SIM pools

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

The picture shows: In the past, the birth of the platform that used SIM pool to complete malicious registration and code reception was like a cybercrime ecosystem "trading platform", and its value was generated between two specific Internet cybercrime ecosystem chain nodes.

Account resources are the most upstream and basic needs of many threat actors, and a large number of card source card dealers can directly sell the value of mobile phone cards online to a large number of midstream account dealers through the SMS verification-code receiving service, achieving high returns.

Account providers can directly obtain the phone number and verification code through the web page of the SMS verification-code receiving service. There is no need to buy a mobile phone card and related equipment to complete the account registration.



Malicious registration through a code-receiving platform

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

The picture shows: Using the SMS verification-code receiving service to complete malicious registration. The SMS verification-code receiving service is responsible for connecting card merchants and groups with mobile phone verification code needs, providing software support, business settlement and other platform services, and making profits through business sharing, usually around 30%.

In November 2016, Aima, the largest SMS verification-code receiving service at the time, was investigated by the police and more than 7 million illicit SIM cards were seized. Since then, many SMS verification-code receiving services have gone underground, and some platforms have also taken measures such as closing new user registrations to reduce risks. Taking the code-receiving platform Ailezan as an example, it closed new user registration in January 2018, making it difficult to find a platform number one, and its platform account even reached 100 yuan each.

There are currently many code-receiving platforms in the market, and the more active ones include: Huoyun, Ailezan, ema666, 60-code, thewolf, Maize, etc.

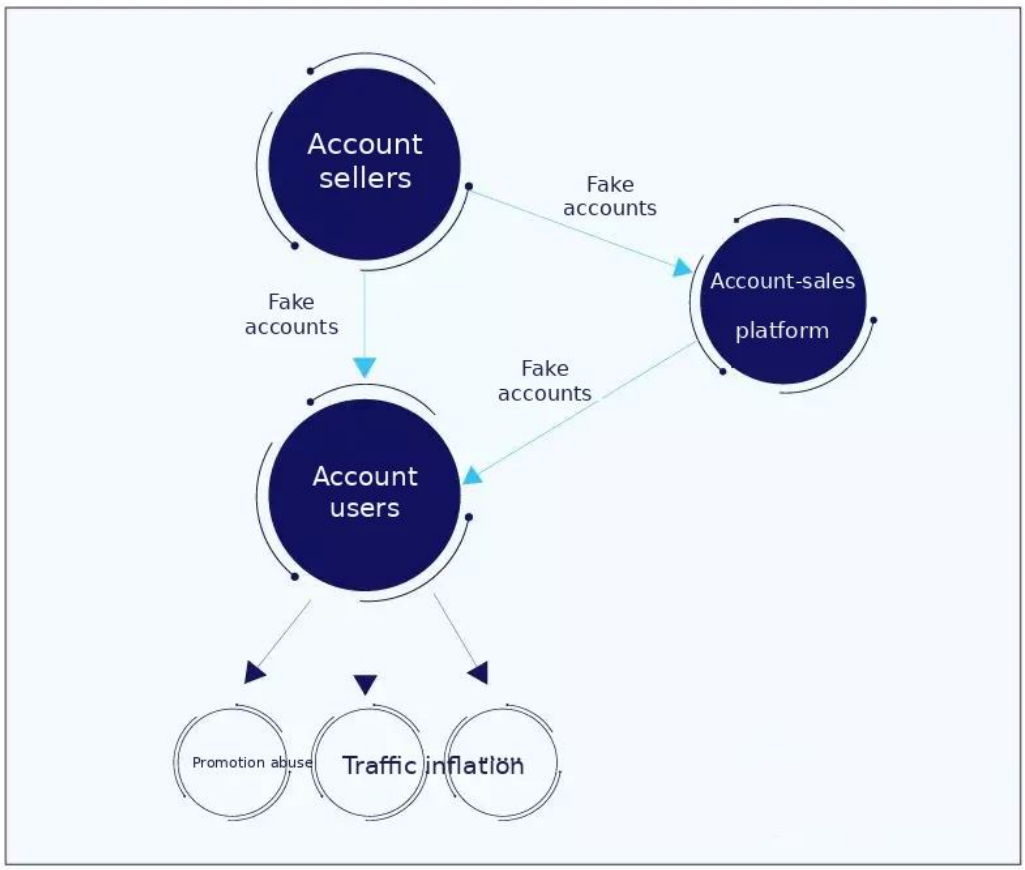
With the upgrade of verification code confrontation, registration projects are no longer verified through a single SMS. Some require voice verification, and some require secondary verification, which requires the registered user to use the registered phone number to send a verification SMS to a designated number. The SMS verification-code receiving service has also been continuously upgraded to keep up with market changes, and has derived services for receiving voice verification codes, retrieving numbers, and sending text messages.

2.2.2 Card issuance platform - improve the efficiency of cybercrime ecosystem account transfer

The card issuance platform is a platform for automated transactions of digital goods. After the account dealers complete the registration of a large number of accounts, they will sort out the malicious accounts and list them on the card issuance platform for direct online bulk purchase by account users in the lower reaches of the industry chain.

It's like buying a phone recharge card on an e-commerce platform, but in terms of application scenarios, the card issuance platform has now become the main transaction channel and collaboration platform for the cybercrime ecosystem of the Internet.

Account users will purchase corresponding fake accounts through the card issuance platform based on their own malicious activity scenarios, which are used for profiteering, platform traffic manipulation, account fraud and other scenarios.



Account trading through account-sales platforms

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

Pictured: Using the card issuance platform to complete account transactions. According to Threat Hunter’s long-term monitoring and resource statistics of cybercrime ecosystem, there are currently more than 10,000 cybercrime operators involved in card issuance platform transactions, involving nearly thousands of types of goods, the number of goods exceeds one million, and the annual output value is hundreds of millions of yuan.

In addition, by tracking the prices of gray goods on the card issuance platform, we found that price is a very intuitive factor that reflects the effectiveness of corporate fraud-control strategies and

changes in market demand. The higher the commodity price, the more effective the corporate fraud-control strategy is, making the cost of cybercrime ecosystem malicious activity higher. At this time, combined with other data, if it is found that attacks launched by threat actors have not decreased, then the reason is that the benefits are still higher than the costs, and then companies need to continue to fight.

2.3 Main measures for enterprises to deal with malicious registrations

2.3.1 Prevention and control-timely capture of the cybercrime ecosystem behavior

In the offensive and defensive battle between the entire enterprise and cybercrime ecosystem, different business scenarios of different enterprises will make the entire offensive and defensive pattern different. However, the core resource of cybercriminal groups are always the fake accounts it controls. As long as cybercriminal groups can be effectively controlled at the point of malicious registration, the overall risk of corporate business fraud controls will be relatively controllable.

Identifying the cybercrime ecosystem resources cybercrime ecosystem relies heavily on the basic resources it holds when committing crimes and monetizing them, including but not limited to phone numbers, IPs, equipment, etc. These the cybercrime ecosystem resources are completely black data for enterprises. If they can match these data with their own business data, they can directly identify malicious accounts or cybercrime ecosystem malicious behaviors, and carry out targeted fraud controls.

Analyzing threat-actor tools cybercriminal groups' attack tools carry cybercriminal groups' attack logic and exploited enterprise business vulnerabilities. By monitoring and reverse engineering the tools, enterprises can learn which business logic vulnerabilities exist or which fraud-control strategies have failed, thereby improving the efficiency of the entire offensive and defensive confrontation.

Monitoring changes in cybercrime ecosystem transactions. The changes in cybercrime ecosystem transaction categories and prices can reflect the effectiveness of the company's fraud-control strategy within a certain period. For example, even if a company has launched a fraud-control strategy, cybercriminal groups can still complete the registration of malicious accounts at a very low cost, which means that the company's fraud-control strategy has failed; on the other hand, if it is found that the transaction price of cybercriminal groups have become higher, reflecting the increase in the cost of cybercriminal attacks, it can be seen that the company's fraud-control strategy has had a certain effect. Effective risk assessment can better promote the implementation and iteration of business security.

2.3.2 Early Warning - Risk warning for fake accounts

The Threat Hunter business intelligence and early warning platform starts from the entire industry chain of cybercrime ecosystem malicious registration, and can monitor and provide early warning for different stages of malicious registration, helping enterprises discover and control the current status of fake accounts they face.

New malicious registration project: cybercrime ecosystem. Before implementing malicious registration behavior, you must first create a new project on the corresponding platform. The act of

creating this project is a signal that cybercriminal groups are about to launch an attack. By monitoring this information, we can obtain the latest trends in the cybercrime ecosystem at any time.

Ongoing malicious registration behavior: The automated tools used by cybercrime ecosystem to initiate malicious registration, the malicious resources used, and the attack interfaces are all paths that expose the attack logic. This information can be used to restore cybercriminal groups attack logic in a timely manner and carry out effective fraud controls.

Risk of malicious account reselling: After completing the registration at cybercrime ecosystem, the fake account is usually placed on the card issuing platform for transactions.

Threat Hunter intelligence and early warning can monitor the new or delisted transaction information and price changes of cybercrime ecosystem fake accounts in real time, helping companies understand changes in cybercriminal groups attack trends and the effectiveness of their own fraud controls.

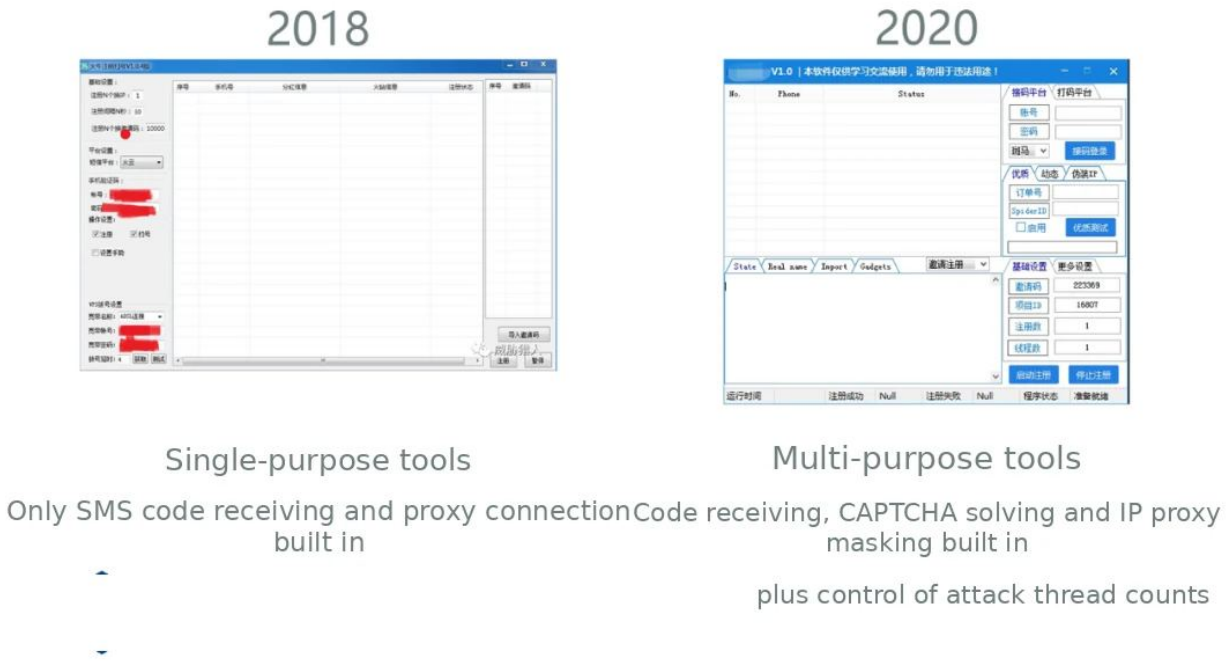
3. The way of conducting malicious activity evolves from automated tools to human-in-the-loop crowdsourcing

3.1 The evolution of trends in cybercrime ecosystem malicious methods

Standing at the time point of 2020, we review the trends of threat actors in the past two years and find the trend of threat actor attacks:

3.1.1 The deeper integration of threat actors’ tools and industry chain

After a long period of technical upgrades, the threat actors tool has been able to integrate multiple functions such as code reception, coding, broadband speed dialing, and network agents in a single tool to bypass business security fraud controls nodes, rather than just combining the CAPTCHA-solving service and the network agent module. By integrating multiple functions, threat actors can use tools to achieve more customized and functional malicious activity behaviors. Today's threat-actor tools are more integrated and have a greater impact.



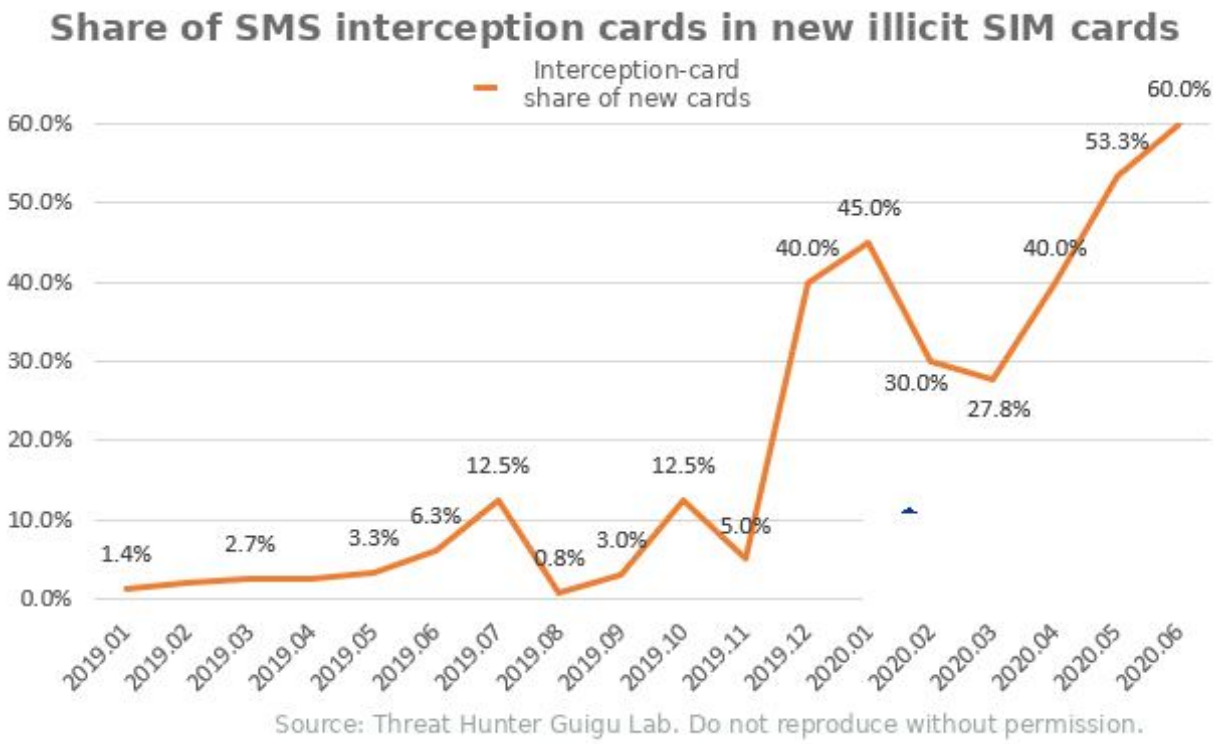
Threat-actor tools in 2018 and 2020: from single-purpose to integrated

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

Pictured: Changes in threat-actor tools

3.1.2 Hiding attack behavior in normal user behavior

Compared with the past, threat actors have begun to use mobile phone SMS interception cards and instant IP dialing to bypass business security fraud-control models to achieve attacks. These two attack methods have one thing in common, which is that the resources used are shared with normal users, which results in the behavior not being judged as threat actors under the general fraud-control model.



Share of SMS interception cards in new illicit SIM cards, 2019–2020

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

The picture shows: The change in the proportion of the increase in SMS interception cards to the total increase in illicit mobile SIM cards. For attacks that can obtain high profits, threat actors have also begun to use crowdsourcing tasks to issue registration tasks and obtain a large number of real-name authenticated accounts at a relatively low price.

In essence, human-operated fraud stems from human greed and laziness. The driving factor is the long-term offensive and defensive confrontation between Internet technology and enterprises and the cybercrime ecosystem, which has evolved into such a relatively advanced form of malicious activity. The next chapter will provide an in-depth analysis of human-operated fraud, so I won’t go into details here.

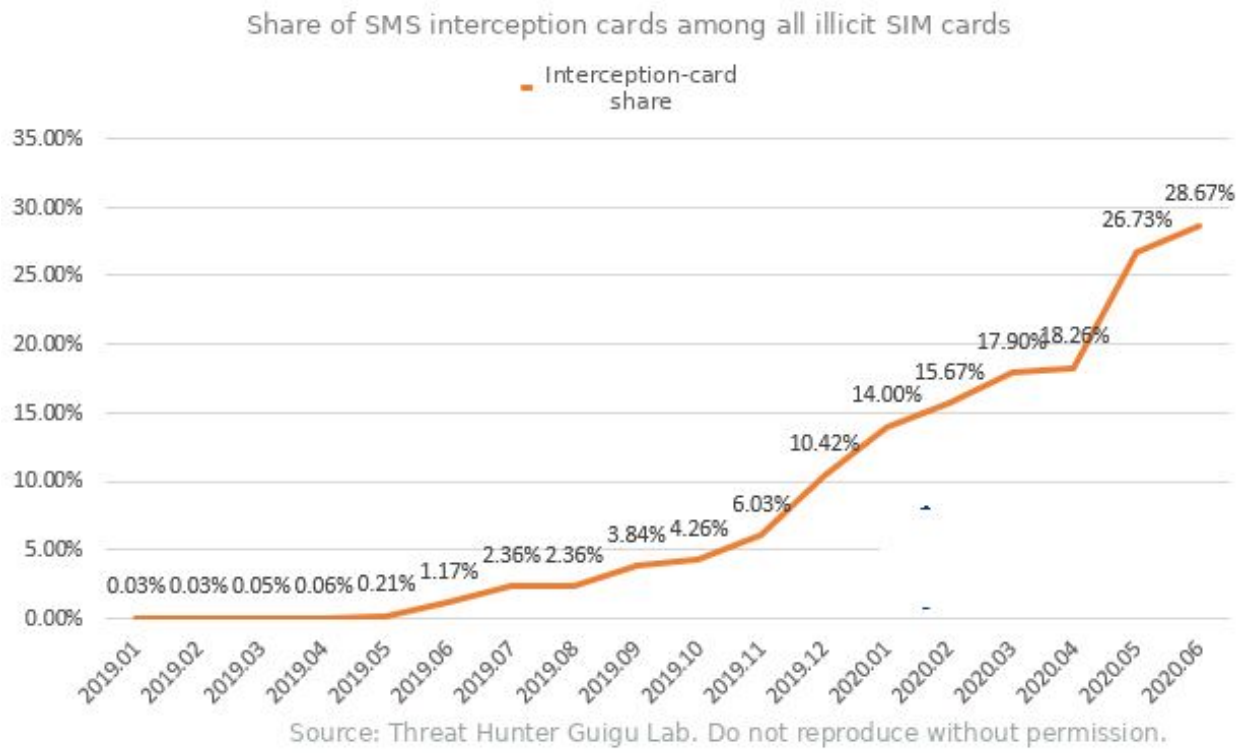
3.2 Changes in threat actors’ malicious methods

3.2.1 Changes in phone numbers - an increase in the proportion of SMS interception cards

At the business security level, identifying malicious phone numbers held by threat actors is a protracted battle. Using the existing phone number information of threat actors, it is generally possible to intercept the phone numbers of threat actors. Faced with the defense from business security, threat actors have also made more or less improvements to the phone numbers they hold: newly purchased phone numbers first use their "clean" identities to register high-profit accounts, and then package high-net-worth accounts after the registration is completed and package them for downstream middle- and low-net-worth threat actors to exploit, thereby squeezing the value of a phone number. However, because threat actors still need to perform the work of maintaining accounts, coupled with the improvement in the efficiency of recycling these number segments by operators, the available value of newly purchased phone numbers has gradually depreciated.

As some domestic mobile phone companies have launched a large number of products for the low-end market and for markets outside China in recent years, threat actors have discovered opportunities that can be exploited. threat actors implant Trojans that can intercept mobile phone text messages into these models, use the phone number of the mobile phone holder to obtain text messages, and then transmit them to threat actors through the network, thereby using the phone number to make profits.

Illicit SIM cards such as SMS interception cards were first discovered at the end of 2018. Because they are more concealed than other channels, the actual time of appearance may be earlier than the time of first discovery. In May 2019, there was an explosion of growth in the number of interception cards, and the platform gathered together. Thanks to the stimulation of malicious registration market demand, interception cards have grown rapidly. Afterwards, threat actors continued to supplement relevant "card sources", allowing interception cards to occupy their own place in the illicit SIM-card market.



Share of SMS interception cards among all illicit SIM cards, 2019–2020

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

The picture shows: Statistics on the proportion of text message interception cards among illicit SIM cards. In this malicious activity scenario, because the holder of the phone number is an ordinary user, the phone number will not be judged as a phone number held by threat actors under normal circumstances. When threat actors use their phone numbers to maliciously register, the general business security system will not judge it as a registration behavior of threat actors, and threat actors can make profits through this "loophole".

3.2.2 human-operated fraud chaos - new customer benefits are maliciously earned by cybercrime ecosystem and promotion-abuse groups

In addition to using illicit SIM cards to register in batches that need to be guarded against, the new customer benefits of some platforms may also be earned by threat actors.

In order to better attract new users, many platforms in vertical fields will issue some high-value benefits such as gift cards, phone bills, and platform gifts to these new users within the platform. In order to defend against malicious attacks by threat actors on the welfare of new users, some platforms will force users to undergo real-name authentication before receiving gift packages. This method does directly prevent threat actors from using tools to automate registration to make profits, but it cannot prevent human-operated fraud from real users who authenticate and then resell their accounts.

Fundamentally speaking, the welfare of new users is generally discovered by some common promotion-abuse users, and then posted to "professional promotion-abuse" communities such as Qiankeba for sharing. The losses of the platform here are still controllable. If the benefits distributed are third-party gift cards or platform gift certificates that can be monetized

downstream, threat actors will be attracted to invest costs and use human-in-the-loop crowdsourcing to make profits.

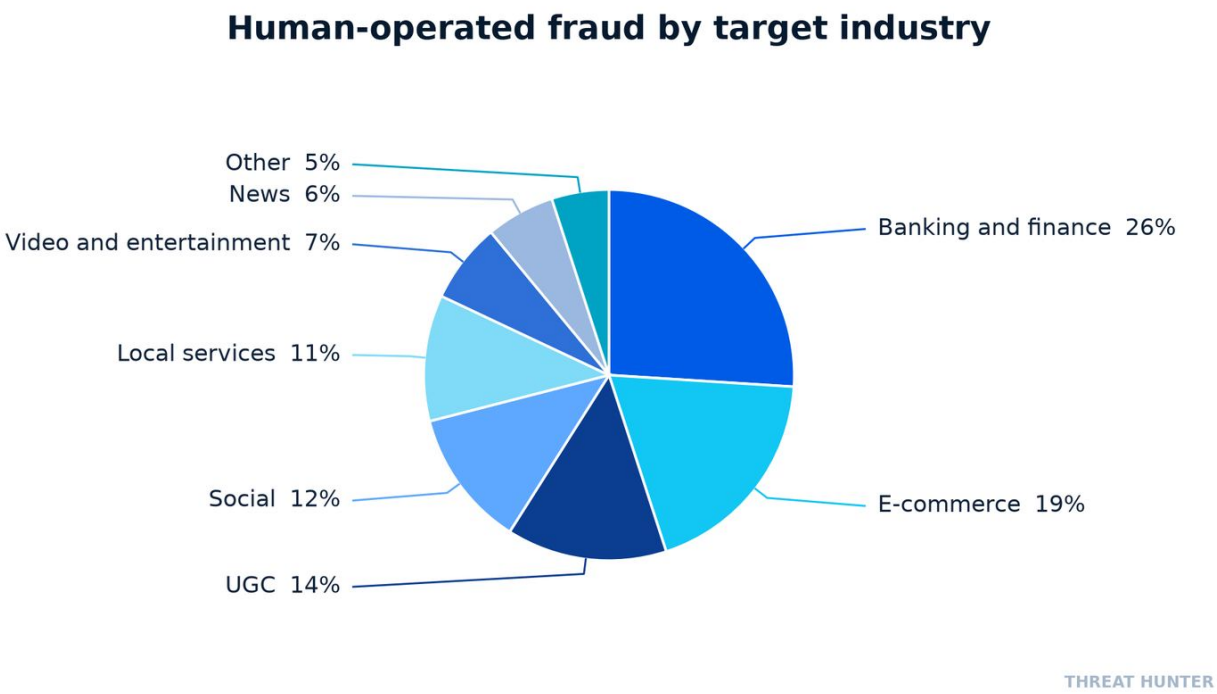


Screenshot of a human-operated fraud crowdsourcing app

Source: Threat Hunter original report, page 19. Original image retained.

The picture shows: Screenshot of a human-in-the-loop crowdsourcing application. According to the detection on Karma, the target industries for human-operated fraud mainly include the following sectors. Banking and finance, e-commerce, UGC platforms and social platforms have become the main targets of threat actors. According to Threat Hunter’s estimates, the human-operated fraud industry generates approximately

The reward amount of 2 billion yuan was lost, and the completed amount of 1 billion yuan was lost, directly causing billions or even tens of billions of losses to the target platform.



Target industries of human-operated fraud: banking and finance lead with 26%

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

Pictured: Proportion of industry types targeted by human-operated fraud

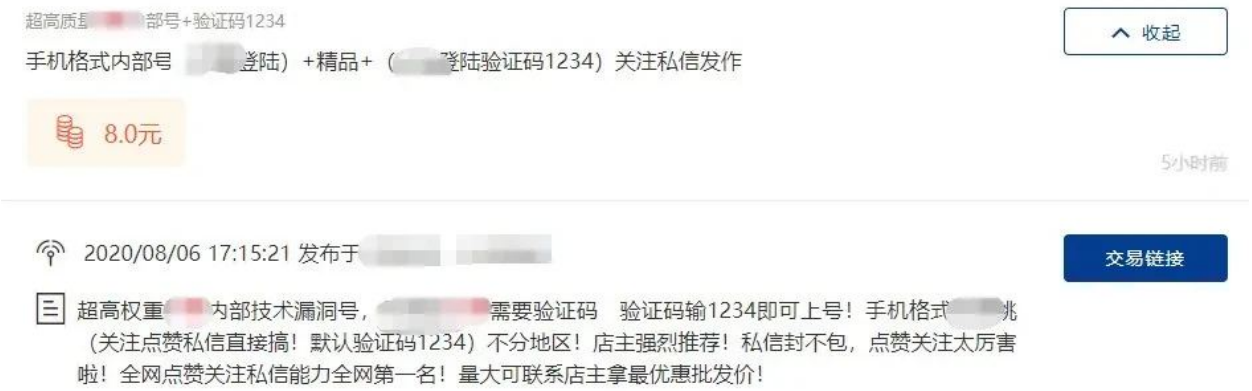
3.2.3 Hidden upgrade of traffic manipulation method - from fake broiler to real broiler

Traffic fraud has always plagued the Internet advertising industry. This is due to the pay-as-you-go settlement method of Internet advertising. This amount includes both clicks and exposure. Because of these quantitative indicators, some unscrupulous advertising platforms have adopted some methods to manipulate ad clicks and ad exposures, and achieve ad reach indicators through fake means to obtain advertising fees.

In the past, Internet advertising traffic fraud usually involved a specialized traffic manipulation studio to receive orders, using clone tools and IP proxy tools to disguise themselves as a large number of devices for traffic manipulation. This traffic manipulation method can be clearly discovered through IP portraits in the current fraud-control system, and its IP is generally a proxy IP.

Nowadays, there are many ways to increase advertising volume. Some webpage advertisements use hidden floating layers to increase ad volume, some software advertisements use malicious pop-ups to increase ad volume, and niche broadband is used to hijack broadband pop-up windows to increase ad volume. Through this method, these platforms and advertising companies can make a lot of money, and only the advertisers will be taken advantage of.

With the development of social media, advertising traffic manipulation has set off a new trend on social media. On the Karma business intelligence platform, we can see that some threat actors are selling some social media accounts, claiming that the accounts are internal vulnerability numbers of the platform, and traffic manipulation them can quickly rise to the top of the trend list.



Threat-actor listing linked to social-media traffic inflation

Source: Threat Hunter original report, page 21. Original image retained.

Pictured: Intelligence on threat actors associated with social media traffic manipulation

3.3 Possible solutions to new threat actors

3.3.1 Abuse of interception cards and other illicit SIM cards

Business security offense and defense have long been based on "human-machine identification" in the past. threat actors use fake people, fake equipment, and fake numbers. Gradually, threat actors began to use real mobile phone devices, and now human participants’s phone numbers and IP resources are also used on a large scale.

This undoubtedly brings more challenges to business security attack and defense. When the determination object is held by both good and bad people, the difficulty of identification, the risk of misjudgment, and customer complaints become more severe.

In the face of illicit SIM cards such as interception cards, it is necessary to distinguish whether they are being used by threat actors based on "whether it is operated by the cardholder himself". This needs to be determined based on the characteristics of the interception card itself and the characteristics of the attack process using the interception card:

1) Set the judgment rules through your own business scenarios. 2) Make a judgment based on the frequency of interception cards and the number of hits on illicit SIM cards and malicious IPs.

3.3.2 How human participants conduct malicious activity through crowdsourcing

The malicious activity performed by human participants's crowdsourcing is mainly done by publishing crowdsourcing tasks. If we want to deal with it, we first need to know the malicious activity process. The above is a textual description of the human-in-the-loop crowdsourcing fraud process. For the sake of convenience, here is a short video application human-operated fraud crowdsourcing task, so that you can intuitively experience the process of threat actors issuing human-in-the-loop crowdsourcing fraud tasks.



Task flow of a short-video crowdsourcing job

Source: Threat Hunter original report, page 22. Original image retained.

The picture shows: A short video crowdsourcing task process where human-operated fraud can be analyzed jointly from the intelligence dimension and the data dimension to accurately locate human-operated fraud accounts:

1) Information from the intelligence dimension. Knowing where the fastest gift collection process is recorded can help us directly erase the information gap between us and threat actors and seize the initiative in the shortest time.

2) The data dimension can be used to make composite judgments using features such as remote login and remote login equipment to discover the action characteristics of threat actors and promptly discover accounts controlled by threat actors.

3.3.3 Countermeasures against traffic manipulation

For advertising publishers, statistical code is generally used to perform data statistics on relevant advertising placements. At this time, the malicious traffic manipulation behavior was discovered through the page statistics function that comes with the statistics code:

1) Find traffic manipulation requests through the length of stay

2) By detecting the IP, you can find out whether the access comes from the traffic manipulation studio, so as to clean out a relatively clean user access list.

The solution for traffic manipulation up on social platforms is more inclined to combine the analysis with the positioning method of human-operated fraud. Through the intelligence dimension and

data dimension, it can discover the accounts controlled by threat actors for traffic manipulation up, and then catch them all according to the characteristics:

1) Information from the intelligence dimension, by understanding the operating points where threat actors can perform traffic manipulation, monitor relevant links, and intercept requests from malicious mobile phone cards and malicious IPs.

2) The data dimension can be used to make composite judgments using features such as remote login and remote login equipment to discover the action characteristics of threat actors and promptly discover accounts controlled by threat actors.

4. In-depth analysis of human-operated fraud

Human-operated fraud has become the most common, most difficult to defend, and extremely damaging to the fraud-control system in the cybercrime ecosystem, a form of malicious activity that infringes on the overall security and stability of the platform. In hidden corners, it causes harm to the platform all the time. Based on long-term investigation and research on the human-operated fraud industry, Threat Hunter deeply analyzes all aspects of this industry, analyzes the development, current situation, harm and defense ideas of the human-operated fraud industry, and strives to present its full appearance from the most professional and comprehensive perspective. This part is mainly divided into the following key points:

1) After several years of development, the models and forms of cybercriminal groups have become more diverse and richer, and have penetrated into many scenarios and industries;

2) human-operated fraud cybercriminal groups have developed rapidly. From 2014 to 2020, the number of human-operated fraud platforms (apps) has increased nearly 40 times, and the number of participants has increased nearly a hundred times;

3) Compared with automated fraud, human-operated fraud places higher demands on customer fraud controls and security capabilities and brings new challenges;

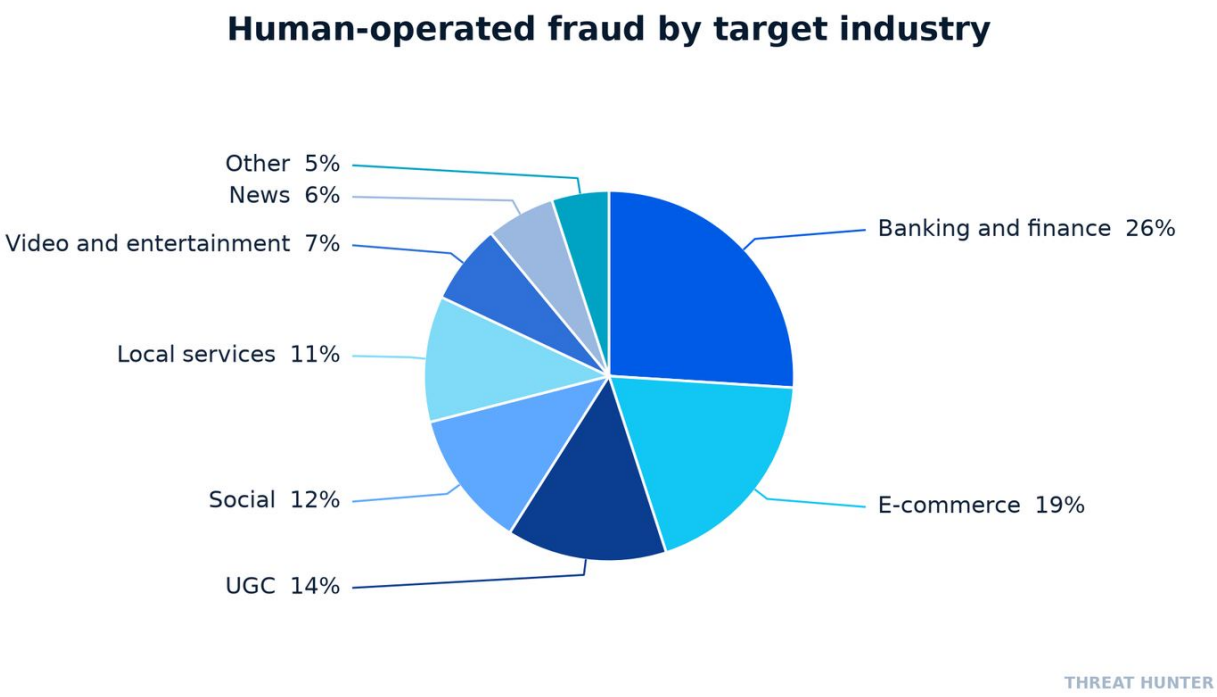
4) Empowering fraud controls with intelligence capabilities and data capabilities is an effective way to identify new fraud patterns.

4.1 Development and Current Situation

In essence, human-operated fraud stems from human greed and laziness. The driving factor is the long-term offensive and defensive confrontation between Internet technology and enterprises and the cybercrime ecosystem, which has evolved into such a relatively advanced form of malicious activity. In recent years, this model and form has become more diverse and rich, from the early single part-time job traffic manipulation orders to today's widespread penetration of multiple industries, multiple scenarios, and multi-tasks; from the early part-time jobs that were only performed on the PC side with a single method, to now mainly on the mobile side; from the early online group media (messaging-app groups, voice chat rooms, etc.) to today's platformization and fragmentation.

4.1.1 Extensive penetration into multiple industries, multiple scenarios, and multiple tasks

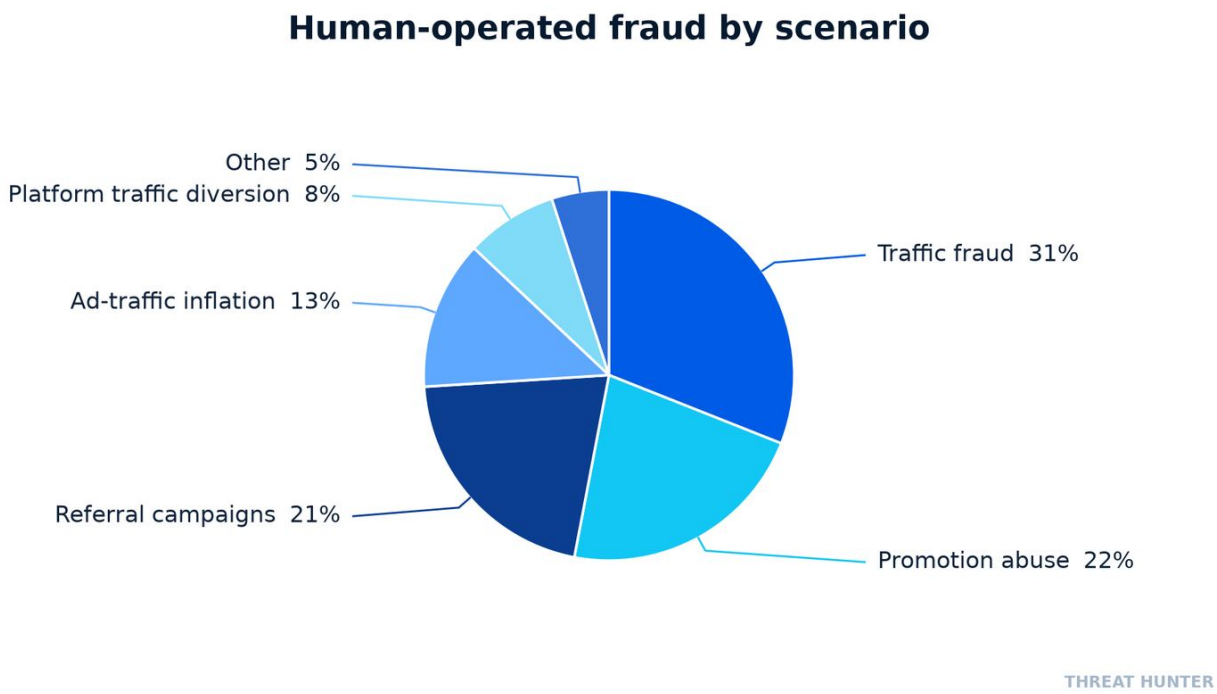
1) Multiple industries involving human-operated fraud involve a wide range of industries, from the financial field to UGC entertainment, from life services, video and audio to news information, social chat, etc., and are involved in everything. As shown in the figure below, it is the proportion of target industry types for human-operated fraud:



Target industries of human-operated fraud: banking and finance lead with 26%

Source: Threat Hunter original report, page 24. Redrawn in English from the original figure.

The picture shows: Proportion of target industry types for human-operated fraud 2) Multi-scenario penetration In terms of business scope, human-operated fraud also covers almost all cybercrime ecosystem malicious activity scenarios, whether it is promotion abuse, traffic fraud, or advertising traffic manipulation, platform diversion, fission promotion and other scenarios, human-operated fraud is involved. See the figure below for specific proportions:

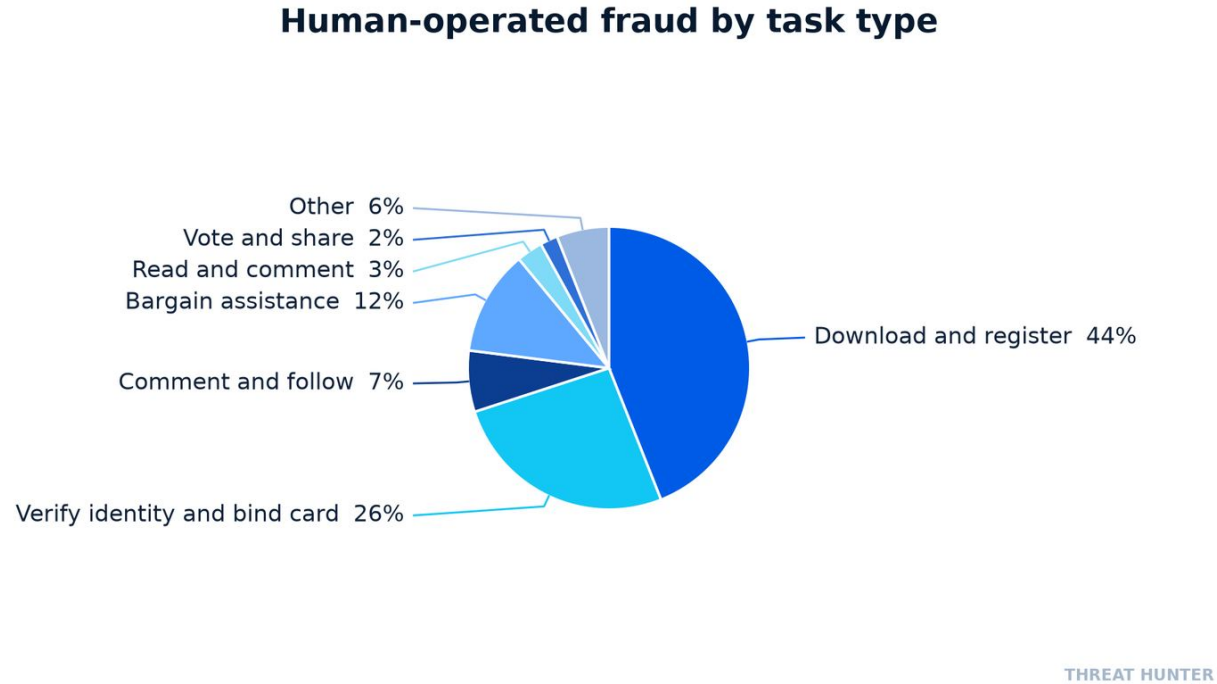


Scenarios targeted by human-operated fraud: traffic fraud is the largest at 31%

Source: Threat Hunter original report, page 24. Redrawn in English from the original figure.

Pictured: Proportion of human-operated fraud scenario types 3) Multi-tasking participation

human-operated fraud tasks are also all-inclusive. All the tasks you can think of that can make profits are affected by human-operated fraud: downloading and registering, authenticating and binding cards, commenting and following, assisting in bargaining, reading and sharing, voting and forwarding, etc., the specific proportion is shown in the figure below:



Task types in human-operated fraud: download-and-register tasks make up 44%

Source: Threat Hunter original report, page 25. Redrawn in English from the original figure.

The picture shows: the proportion of human-operated fraud task types. By counting the titles, contents and keywords of human-operated fraud tasks that have been monitored for a long time, the following word cloud diagram is formed. It can also be seen that the main tasks of human-operated fraud are: download registration, authentication and card binding, comment attention, etc.



Most frequent keywords in human-operated fraud tasks: register, download, verify and follow

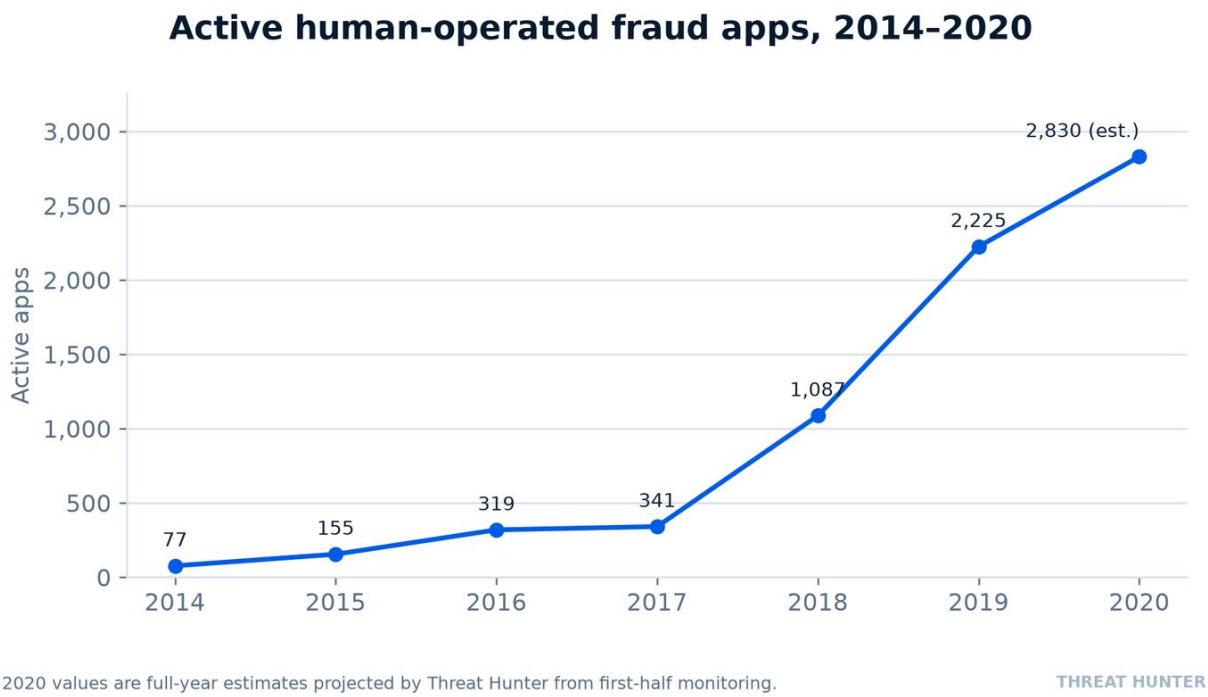
Source: Threat Hunter original report, page 25. Redrawn in English from the original figure.

Pictured: word cloud of human-operated fraud task types

4.1.2 Human-operated fraud apps have developed rapidly in recent years 1) app activity and downloads increased exponentially from 2014 to 2020

In the earliest days, human-operated fraud still used "online groups" as a medium to communicate and disseminate information. Typical examples include voice chat groups, messaging-app groups for underground cybercrime communication, forum chats, etc. However, when the Internet became mobile, human-operated fraud also kept pace with the development of the times.

Threat Hunter has monitored that from 2014 to 2020, the number of human-operated fraud apps has increased exponentially: there were less than a hundred in 2014, and nearly 3,000 this year, as shown in the figure below:

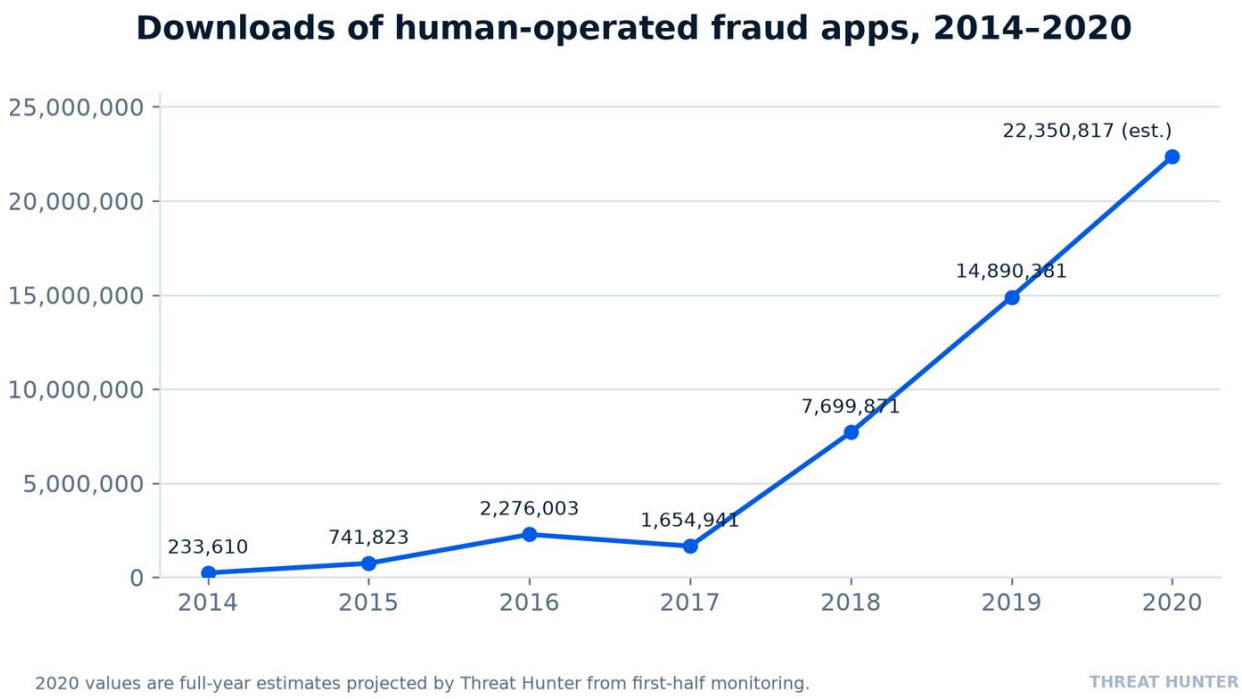


Active human-operated fraud apps, 2014 to 2020: from 77 to an estimated 2,830

Source: Threat Hunter original report, page 26. Redrawn in English from the original figure.

The picture shows: The development trend of the number of active human-operated fraud apps from 2014 to 2020 (Note: The number of active human-operated fraud apps in the first half of 2020 was 1,415. Based on the number in 2019 and the development status of human-operated fraud, we reasonably speculate that the number of active human-operated fraud apps in 2020 reached 2,830.)

When the number of active human-operated fraud apps is growing exponentially, the number of related downloads is also growing rapidly:

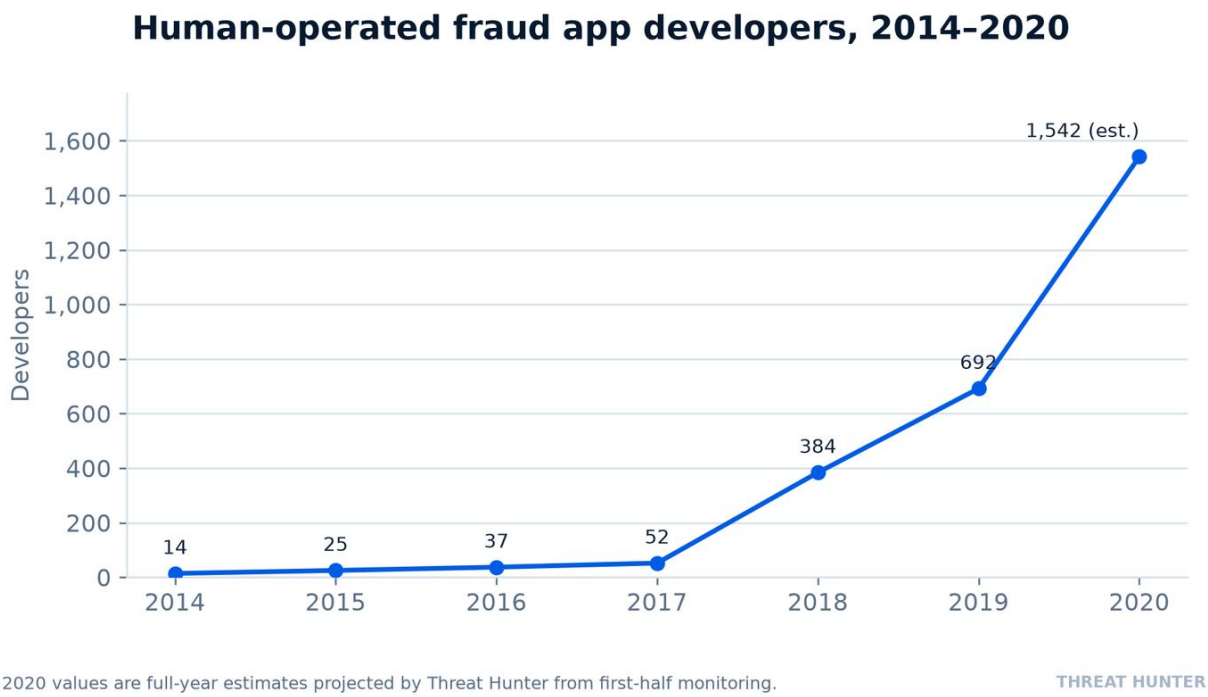


Downloads of human-operated fraud apps, 2014 to 2020: an estimated 22.35 million in 2020

Source: Threat Hunter original report, page 27. Redrawn in English from the original figure.

The picture shows: The development trend of the number of downloads of human-operated fraud apps from 2014 to 2020 (Note: The number of downloads of human-operated fraud apps monitored in the first half of 2020 was 12,350,817 times, based on the number of downloads in 2019 Based on the volume and the development status of human-operated fraud, we reasonably speculate that the number of downloads of human-operated fraud apps can increase by another 10,000,000 times in the second half of 2020, and the final number of downloads for the whole year will be: 22,350,817 times.)

2) The rapid growth of developers from 2014 to 2020. Behind the explosive growth of the number of human-operated fraud participants is inseparable from the support of resources. One of the important resources is the platform: the human-operated fraud platform—that is, the human-operated fraud app. This aspect can be reflected in the number of developers of human-operated fraud apps. In Threat From the data monitored by Hunter, we can find that the number of developers of human-operated fraud apps has also grown exponentially: from less than 20 in 2014 to about 1,500 this year, the development rate is astonishing.



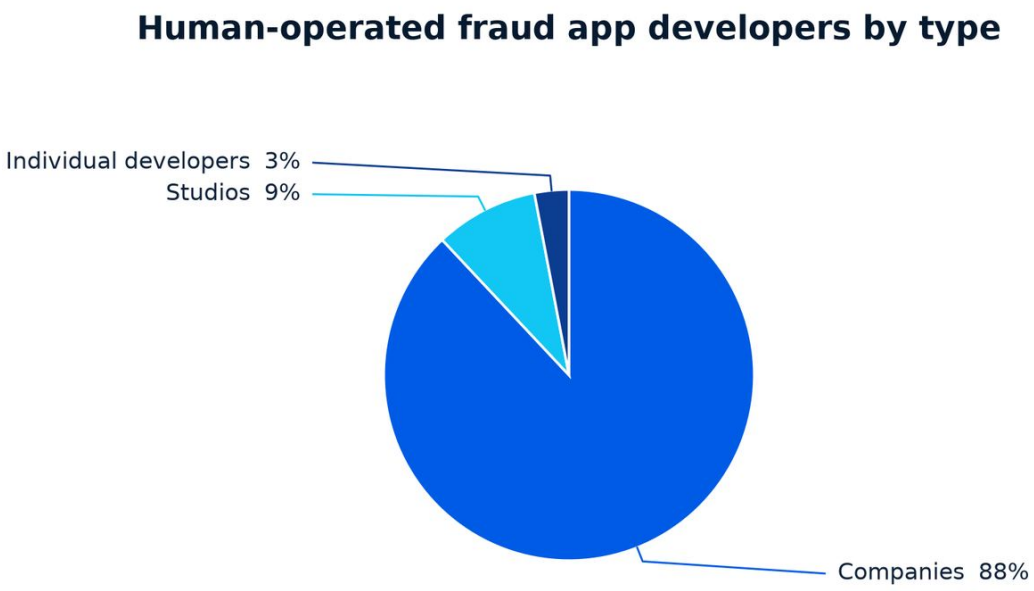
Human-operated fraud app developers, 2014 to 2020: from 14 to an estimated 1,542

Source: Threat Hunter original report, page 27. Redrawn in English from the original figure.

The picture shows: the development trend of the number of human-operated fraud app developers from 2014 to 2020

(Note: The number of human-operated fraud app developers monitored in the first half of 2020 was 771. Based on the development status of human-operated fraud, we reasonably speculate that the number of human-operated fraud app developers reached 1,542 in 2020.)

Among all mobile developers monitored by Threat Hunter, there are 1,407 enterprise developers, accounting for 88% of the total 1,598.

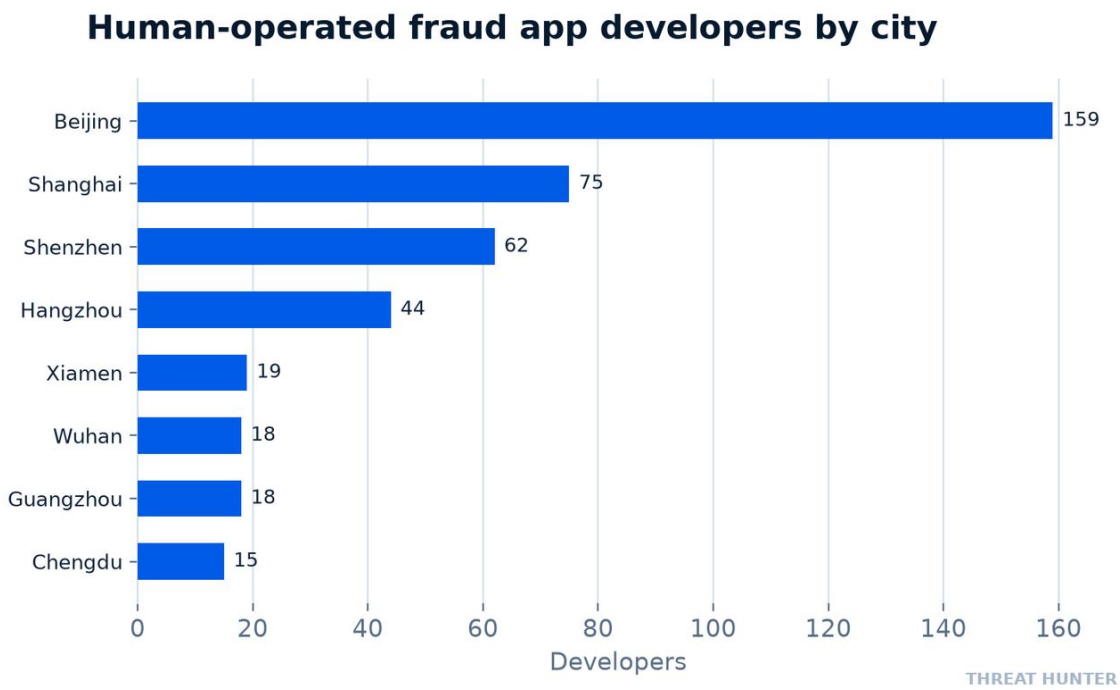


Developers of human-operated fraud apps by type: 88% are companies

Source: Threat Hunter original report, page 28. Redrawn in English from the original figure.

The picture shows: The number of developers of various types accounts for nearly 90% of enterprise developers. The profits of providing human-operated fraud platform services are evident. Because small things lead to big things, this also reflects from the side how profitable the entire human-operated fraud industry is.

The geographical distribution of developers is also basically consistent with the regional development characteristics of China’s Internet. The first four regions are: Beijing, Shanghai, Shenzhen, and Hangzhou:



Developers of human-operated fraud apps by city: Beijing, Shanghai, Shenzhen and Hangzhou lead

Source: Threat Hunter original report, page 28. Redrawn in English from the original figure.

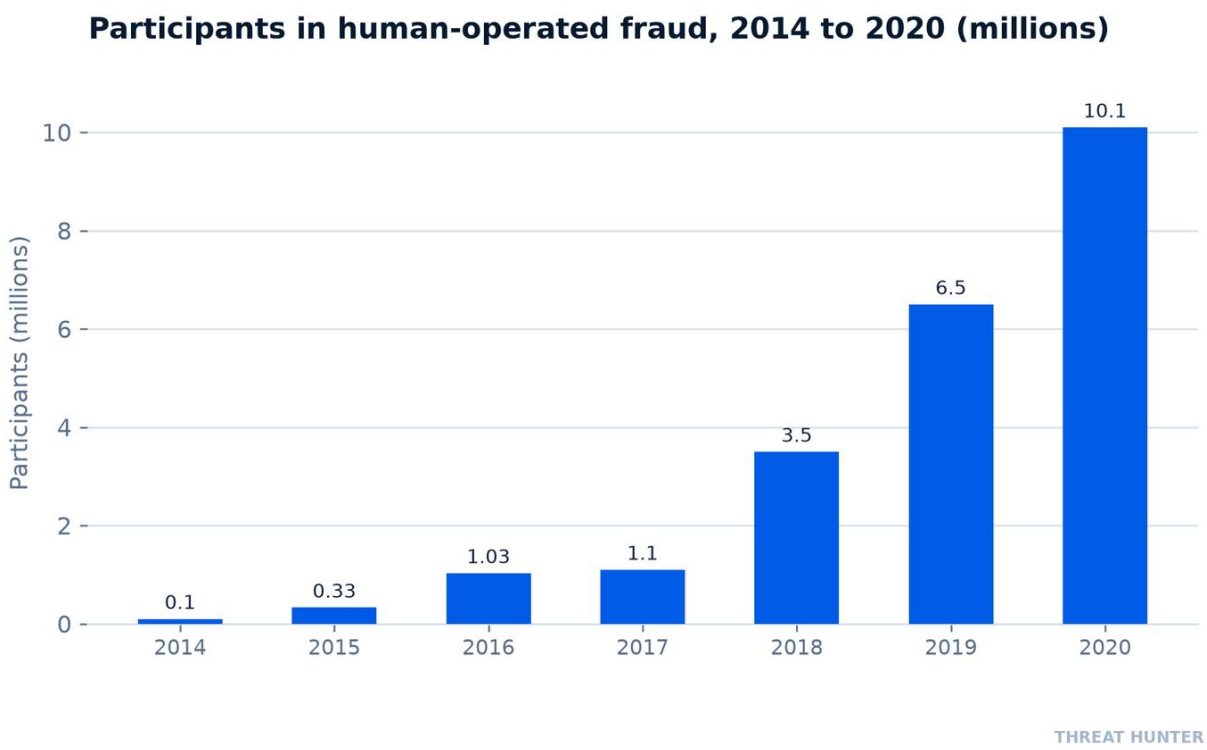
Pictured: City distribution of real-life cheat developers

What's more, some companies have developed many human-operated fraud apps at the same time. For example, a company in Bengbu has developed 23 human-operated fraud apps at the same time; a company in Qingdao has developed 10 human-operated fraud apps at the same time, etc. As the saying goes, if there is no profit, you can’t afford it early. It can be seen that the profits that developing human-operated fraud apps can bring to these companies will not be too little.

4.1.3 Portraits of people involved in human-operated fraud

So, what are the characteristics of users who participate in human-operated fraud?

1) The number of people in the human-operated fraud industry. Whether it is the diversity of human-operated fraud tasks or the vigorous development of apps, it is all driven by huge demand. In fact, the number of users participating in human-operated fraud monitored by Threat Hunter has indeed increased exponentially, from more than 100,000 people in 2014 to a conservative estimate of about 11 million this year, an increase of more than 100 times in seven years. The "power of human-operated fraud" cannot be underestimated:

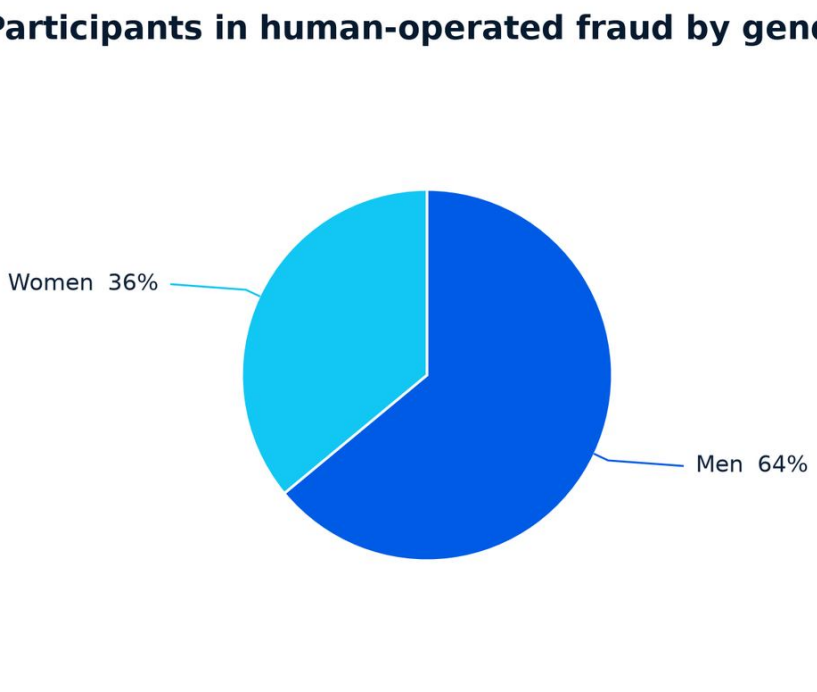


Participants in human-operated fraud grew from about 100,000 in 2014 to 10.1 million in 2020

Source: Threat Hunter original report, page 29. Redrawn in English from the original figure.

The picture shows: The development trend of the number of participants in human-operated fraud 2) The ratio of male to female in human-operated fraud

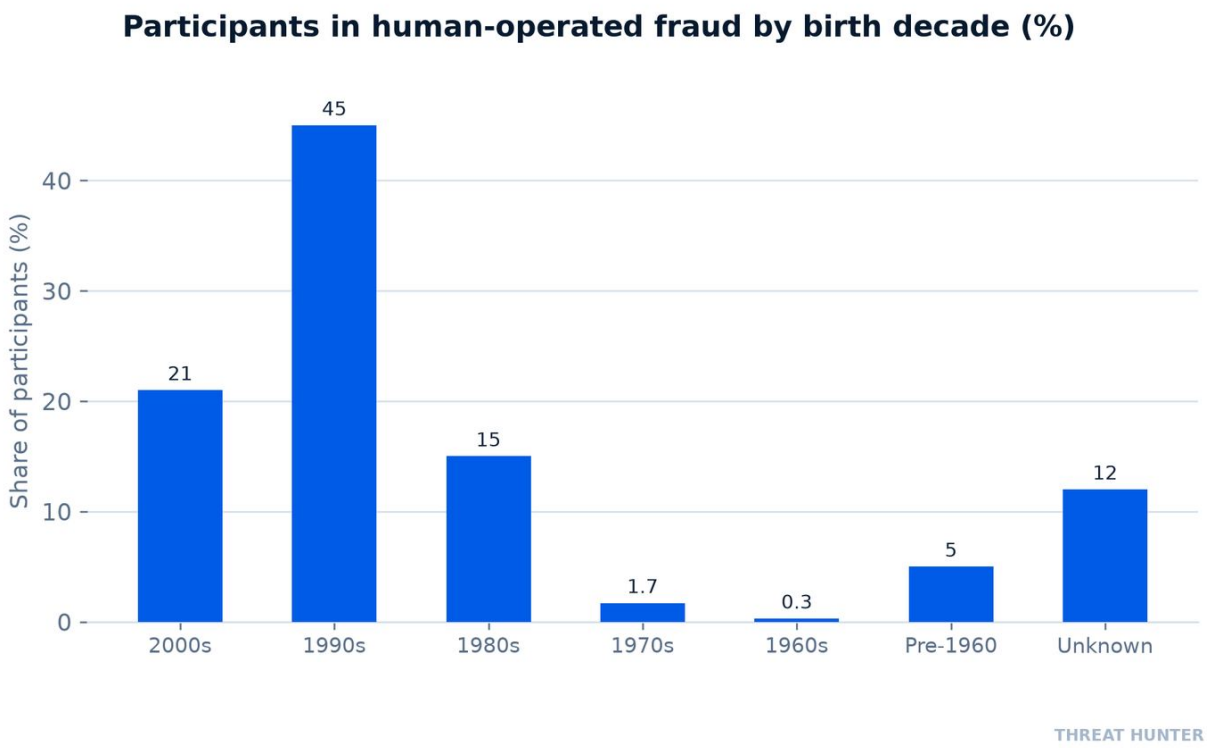
Through a random sampling survey of user groups who participated in human-operated fraud, it was found that the majority of human-operated fraud participants were men, accounting for 64%, and 36% were women:



Participants in human-operated fraud by gender: 64% men, 36% women

Source: Threat Hunter original report, page 30. Redrawn in English from the original figure.

Pictured: Ratio of men and women in human-operated fraud participants 3) Age distribution of human-operated fraud In terms of age distribution, the post-90s generation is the main force in human-operated fraud, accounting for 45%, followed by the post-00s generation and the post-80s generation, accounting for 21% and 15% respectively. It can be seen that people involved in fraud are generally young, which also reflects from the side. The human-operated fraud industry will continue to develop.

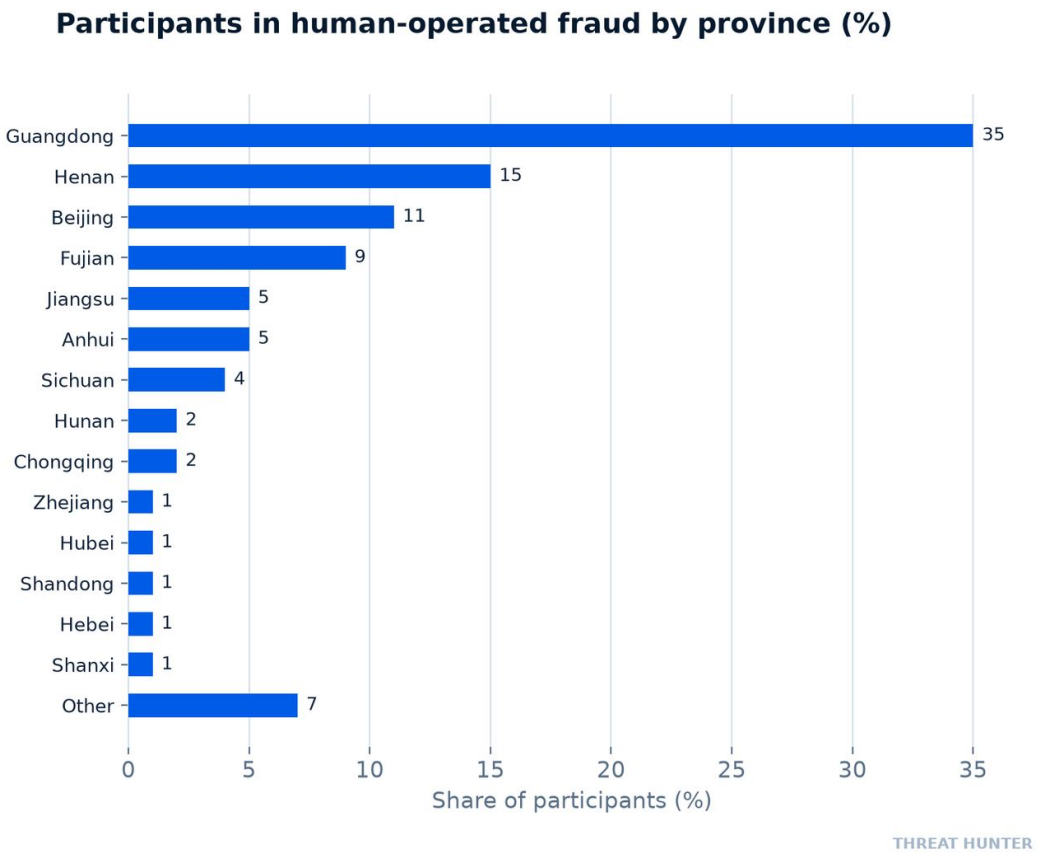


Participants by age group: people born in the 1990s are the main force at 45%

Source: Threat Hunter original report, page 30. Redrawn in English from the original figure.

The picture shows: Age distribution of human-operated fraud participants 4) Regional distribution of the number of human-operated fraud participants

From a geographical point of view, human-operated fraud participants are distributed in South China, East China, North China, and Central China. Among them, Guangdong Province in South China accounts for the largest proportion, reaching 35%:



Participants by province: Guangdong accounts for the largest share at 35%

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

Pictured: Geographical distribution of people involved in human-operated fraud

4.1.4 Statistics on the losses caused by human-operated fraud to the industry

So how much damage has human-operated fraud caused to various industries? Threat Hunter has made comprehensive statistics on human-operated fraud platform tasks in the past six months, and calculated based on the number of bounties, bounty amounts, number of completions, bounty time, completion time and other factors, and the following conclusions have been drawn:

The human-operated fraud industry generates approximately 2 billion yuan in reward amount and 1 billion yuan in completed amount every year, directly causing billions or even tens of billions of losses to the target platform.

4.2 Pain points and hazards

4.2.1 human-operated fraud vs automated fraud

	Human-operated fraud	Automated fraud
Who carries it out	Threat-actor groups plus large numbers of real users	Threat-actor groups
Devices	Real phones	Device farms, cloud phones, emulators
Resources	Real phone numbers, real IP addresses	Illicit SIM cards, illicit IP addresses
Process	Operated by real people	Protocol cracking / simulated operation

Table 3-1: how human-operated fraud differs from automated fraud

Source: Threat Hunter original report, page 32. Redrawn in English from the original figure.

The table shows: Comparison of the characteristics of human-operated fraud and automated fraud

4.2.2 human-operated fraud vs traditional fraud controls

Traditional fraud controls is based on the detection and identification of risky behaviors based on the resources of threat actors and the characteristics of "abnormal people" displayed by groups of threat actors. When threat actors hide behind the scenarios and use cash rewards to mobilize real users to complete fraud tasks, "human-machine recognition" is challenged by "human participants", and traditional fraud controls becomes stretched. The pain points of fraud controls are specifically manifested in the following four aspects:

1) Failure of protection means Whether it is the risk database, risk rule library, risk feature library, etc. at the rule level, or the AI algorithm, decision-making engine, etc. at the model level, the accumulation of knowledge mainly comes from long-term data analysis and precipitation of automated fraud. Traditional risk-management data blacklists such as SIM-pool cards and proxy IPs are completely unsuitable for human-operated fraud scenarios. In addition, characteristics such as behaviors, portraits, and user relationships of human-operated cheaters are often discrete and varied. Although they are not completely traceable, the input of the algorithm model strongly relies on the security personnel's insight and analysis capabilities of risk data and scenarios, which requires very high operating costs.

2) Dealing with Blurred Boundaries Compared with dealing with illegal threat actor accounts, the complexity of dealing with illegal real user accounts has increased significantly. How to reasonably classify and grade the violations of real users, how to integrate fraud-control indicators and user experience, how to provide highly explainable reasons for disposal to the business team, etc. These are further challenges for the fraud-risk team.

3) Risk response lags. Once a human-operated fraud risk event occurs, the fraud-risk team is almost powerless in the early stage and can only allow the scope of the risk event to continue to expand. From the occurrence of risk events to the implementation of countermeasures, the greater the time difference, the greater the losses. In the scenario of human-operated fraud, this time difference is much larger than that of automated fraud.

4) Difficulty in traceability and review

Real users are between threat actors and victim companies, building a natural barrier for threat actors, making it difficult to track and trace the source afterwards. Moreover, from the fraud data that has been mastered, only a limited range of fraud data can be associated and diffused.

human-operated fraud patterns change frequently, making it impossible to effectively transfer knowledge and reuse experience for future human-operated fraud behaviors.

4.2.3 Additional risks brought by human participants fraud

In addition to the common harm caused by common automated fraud (such as promotion abuse, channel abuse, fake users, false orders, etc.), human-operated fraud also introduces the risk of personal information being abused and leaked by threat actors.

threat actors acquire accounts registered by real users and use them for illegal purposes. threat actors induce real users to assist in completing friend-assisted authentication, real-name, face authentication, etc. Not only do real users violate the platform's user terms, they even have to bear potential legal risks.

In addition, when the Threat Hunter security team was investigating the human-operated fraud industry chain, they once conducted an in-depth investigation into a financial bounty task. This task was a "certification and card binding" type task: users only need to successfully bind their cards to get a commission reward of 30-50 yuan.

First of all, from the perspective of income-output ratio, threat actors are willing to pay such a high commission, which means that threat actors' income is likely to reach one hundred yuan or more, so for the financial platform that promotes it, it will inevitably suffer a lot of losses; secondly, when we chatted with the task publisher, we were asked to provide: name + phone number + ID card + bank after completing the task, as shown in the figure below:



Chat with a task publisher asking for personal data

Source: Threat Hunter original report, page 33. Original image retained.

The picture shows: Chatting with the task publisher. Note that after handing these information to the task publisher, you still cannot get the commission. You must complete the last step: give the SMS verification code received on your mobile phone to the task publisher before you can receive the commission. Name, phone number, ID card, bank card and short message

The verification code is very sensitive personal information and is completely exposed to the control of threat actors. The security of personal information and even property is seriously threatened.

4.3 Confrontation and Resolution

Such surging human-operated fraud has various advantages over machines, and it also poses a direct challenge to traditional fraud controls, and the challenges it brings are becoming more and more severe. So, how to prevent and control it?

Threat Hunter believes that intelligence capabilities and data capabilities empower fraud controls and are the solution to the new fraud model of human-operated fraud.

4.3.1 Intelligence Dimension

For example,Threat When Hunter conducted a comprehensive monitoring of the human-operated fraud platform last year, he discovered some tasks with information similar to this: "Register and download XX software, and set the password to a123456. After completing it, contact me for payment." After that, we followed the clues, and in the remaining hundreds of Nearly 100,000 related tasks of the same type were found in a human-operated fraud platform, and their password setting requirements are the same. This obviously shows that the same group is conducting batch registration attacks on this platform. In order to facilitate memory and unified management, task completers are required to set a unified simple password.

After we captured this threat information, we collected intelligence from the entire network and organized key information, including password characteristics, task publisher information, the earliest start time of the task, etc., and then handed over this key information to the social platform as soon as possible.

After receiving our intelligence information, the platform also conducted reverse tracing and positioning as soon as possible. As a result, a large-scale gray production gang was uncovered and successfully attacked, which directly maintained the safety and harmony of the platform and nipped the damage in advance.

4.3.2 Data dimensions

Information from the intelligence dimension can help us directly erase the information gap with threat actors and seize the initiative in the shortest time. However, only intelligence information is ultimately weak. At this time, data information is also needed to locate threat actors and support subsequent mining work. Risk data related to human-operated fraud includes: risk apps, risk equipment, risk accounts, and QR codes, links, tutorials, task processes, etc. for tasks in human-operated fraud.

For example, starting in May this year, a certain domestic payment platform began to engage in activities to attract new customers and link cards to give gifts. Because it involves payment and bank cards, the reward amount is very high, which will naturally be targeted by the cybercrime ecosystem. But after all, this type of activity requires real names, bank cards, etc., and the cost

and threshold for automated fraud are relatively high. Therefore, cybercrime ecosystem with specific channel resources has begun to gain popularity among many human participants.

The fraud platform publishes tasks (after long-term tracking research, we found that some cybercriminal groups have a large amount of cash back resources, which they call "holes").

After Threat Hunter sensed the threat for the first time, it focused on monitoring such fraud methods. On the one hand, it conducted extensive intelligence collection and analysis from the intelligence dimension. On the other hand, based on Threat Hunter's hundreds of millions of device profiling capabilities, it located risky devices and extracted information from human-operated fraud users. In addition, it also delivered data features such as these risky devices, task sharing links, and settlement links to the payment platform.

After receiving the data, the platform conducted matching verification and directly discovered thousands of risky accounts. Later, it located hundreds of upstream master accounts and tens of thousands of downstream risky accounts through the common behaviors and network relationships of these accounts. Threat Hunter further assisted the platform in studying the behavior of these master accounts, and found that these master accounts had been hidden on the platform for a long time, and organized malicious users to exploit promotions whenever they were active.

3. Iteration of offensive and defensive technologies

1. Evolutionary history of group control of threat actors

In the second half of 2018, an equipment company appeared that claimed to be "the best group control on the market" and vigorously promoted its products. It is said that the floor space alone can save 95% compared to traditional group control. We purchased and dismantled a piece of equipment. When we disassembled it, we found that it was a box-type device that needed to be connected to network cables and power cables. We can call it a "box control" for short.

1.1 Group control & box control

Group control is a way to conduct batch attacks by operating multiple mobile phones. It can be said to be a rigid need for threat actors studios. Driven by market demand, suppliers of group control equipment are very good at upgrading and optimizing them using various technologies. The following are photos of group control equipment in a studio.



A room full of box-control devices

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

The figure below shows the protagonist this time - the internal structure of the box control. The screens of twelve Android mobile phones were removed, and the motherboards were integrated into one large motherboard through circuit integration for unified power supply and management.



Inside a box control: phone motherboards integrated on one board

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

As for the number of devices, it cuts each mobile phone motherboard into ten clones by cutting memory. Ultimately, operating one box controller is equivalent to operating one hundred and twenty different mobile phones. Mobile phone equipment that originally required a hall to be stored now only requires a few shelves, significantly reducing the equipment operating costs of threat actors.

In terms of batch operation, the key parameters of most of the enterprise's business interfaces are set with specific algorithms. When it is impossible to directly attack them, threat actors often need to simulate normal user operations by simulating clicks to achieve the purpose of attack. A common simulated click solution is to locate the coordinates that need to be clicked by identifying colors, text, and shapes. This method often requires fault-tolerant judgment, and then determines whether you have clicked into the target page by identifying colors, shapes, etc. Each recognition takes time and is relatively slow.

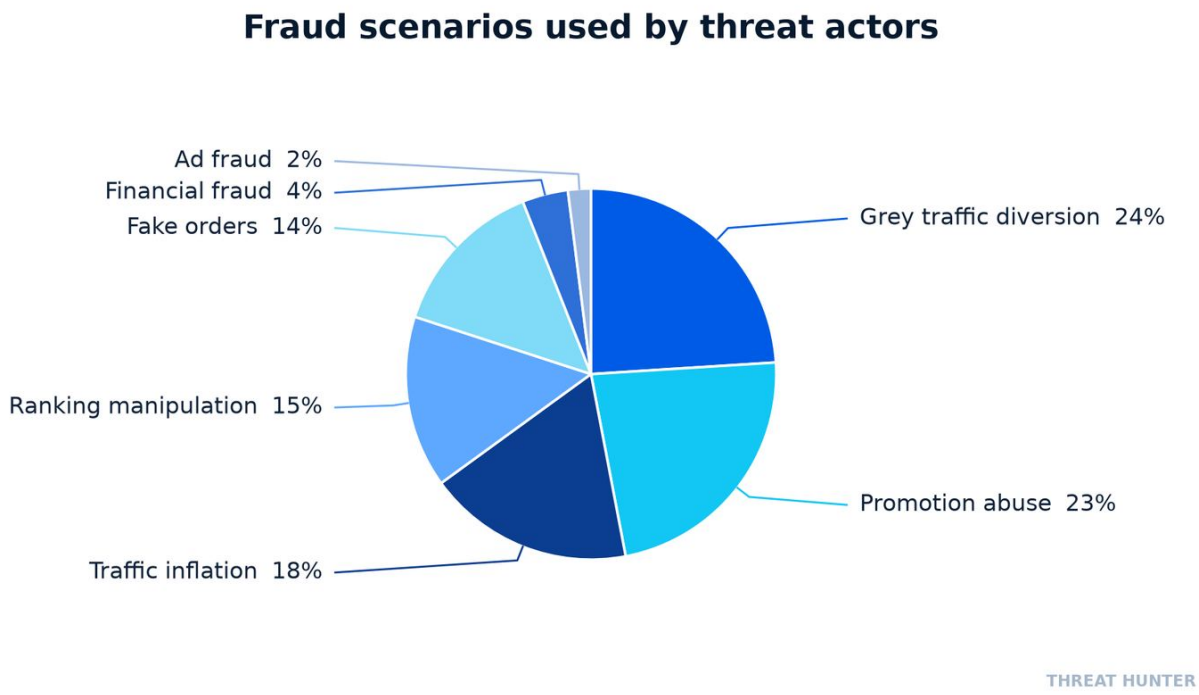
Box Control uses appium, an Android automated testing tool based on the UiAutomator2 testing framework, which directly locates the controls of the app through text, control id, control name, etc., which means that compared with the above method, there is no need to take a screenshot after each click, and there is no need to judge the click position based on the picture pixel by pixel. The speed has been improved, and many companies use appium to complete the automated testing of their own products.

1.2 Evolution of threat actors, optimizing attack efficiency and cost

Recalling the evolutionary variants of "group control" and combining it with various recent events, we find that the current cybercriminal attacks on the Internet have two characteristics:

1.2.1 Sixty percent of attack scenarios are based on quantity.

With the development of the Internet, threat actors have formed some fixed attack patterns and routines. There are a large number of attack scenarios attached to traffic, disguised as normal business, and then make profits through repeated attacks.



Fraud scenarios used by threat actors

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

1.2.2 Heavy reliance on basic resources of threat actors

In the underground market, there are many "resources" with huge and stable demands such as equipment: IP, ID card, bank card, payment account, computer modification tools, automated attack software, sliding verification code, secret monetization channels, etc. They have also gradually formed a "service-oriented threat actors collaboration platform" like a CAPTCHA-solving service. There are more and more of these platforms, forming a huge cybercrime ecosystem basic resource network. Attacks by threat actors also rely heavily on these basic resources.

Threat-actor need	Solution or supporting industry
Batch attacks	Device numbers plus batch operation: group-control devices
Large numbers of IPs not on blacklists	Home-broadband IP pools pooled through soft routers: rapid dial-up and mixed dial-up
Large numbers of distinct device profiles	Fake device data forged with higher privileges and sent to company apps: software and hardware device-spoofing tools
Receiving SMS and voice codes in bulk and sending unblock messages	Third-party platforms provide the service: code-receiving platforms
Passing human-verification checks	Supporting industry: CAPTCHA-solving platforms
Easy trading of basic resources	Semi-open marketplaces: account-sales platforms
Identity data (ID cards and numbers, bank cards and so on)	Supporting group: data brokers
Data trading, cash-out and money laundering (stable channels for monetisation and laundering)	Supporting industry: trading of personal and company payment accounts; online laundering services; the dark web

Threat-actor needs and the solutions that serve them

Source: Threat Hunter original report, page 39. Table re-typeset in English from the original.

The picture shows: threat actors' requirements and corresponding solutions. As the attack and defense logic and upstream service resources tend to be fixed, threat actors have gradually transitioned from the era of iteration of attack and defense logic to the optimization iteration of attack efficiency and cost. Still taking the attack device as an example, let's explore its change process.

1.3 How threat actors solve batch attacks

1.3.1 Box control

Optimization point: Package general-purpose attack tools to provide supporting services, which lowers the operating threshold of attacks. threat actors in group control equipment and service providers have shown a tendency to package and integrate some general-type functions such as dial-up IP and machine modification tools.

With built-in VPN functions, machine modification functions, and virtual positioning functions, as well as cloud backup capabilities, threat actors can upload a set of attack environments together with the accounts logged in to the environment for backup, and switch environments by restoring snapshots to conduct a large number of attacks. Box control also provides memory management and other capabilities, which better meets the goal of group control equipment - reducing operating costs, that is, less manpower can be used to operate more equipment, and the efficiency and frequency of attacks have been effectively improved.

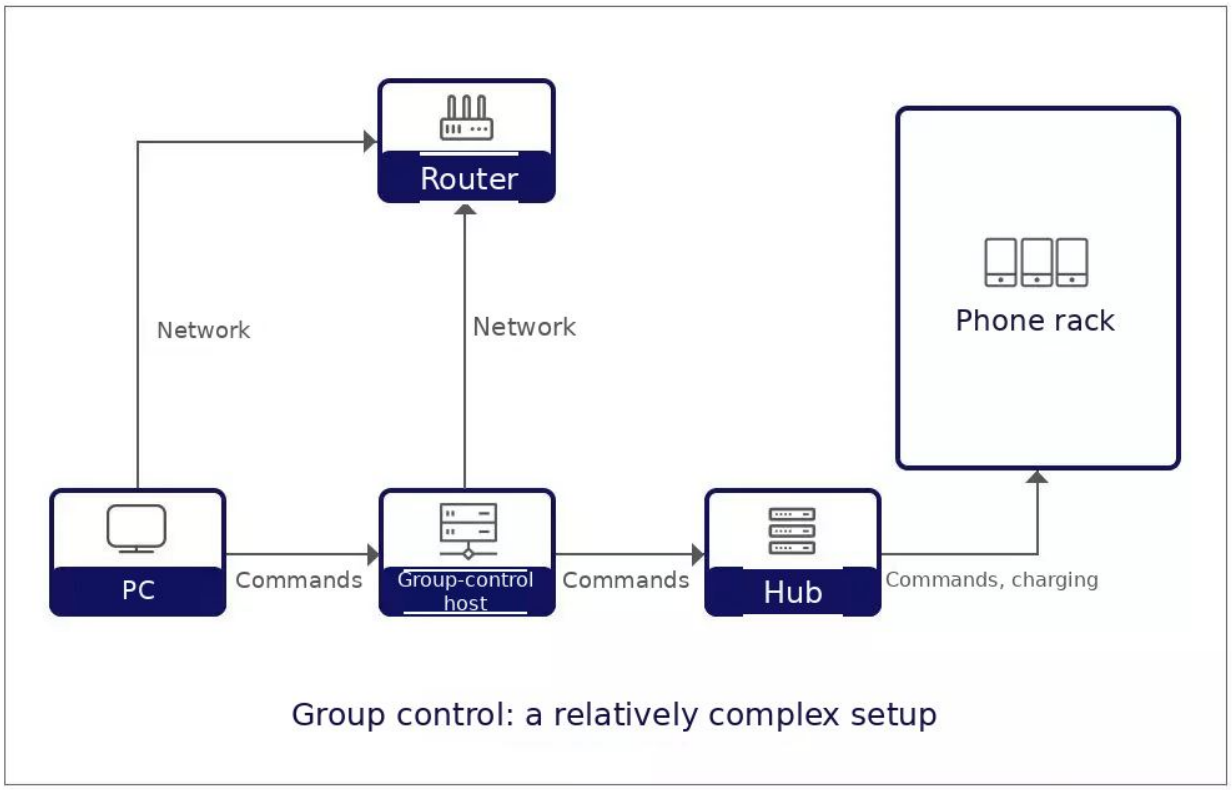


Chart: Threat Hunter

Group-control connection: a relatively complex setup

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

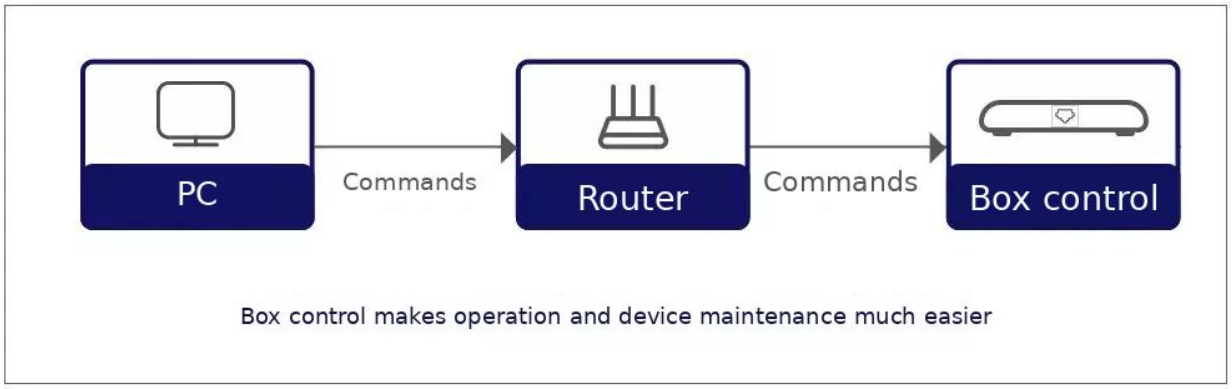


Chart: Threat Hunter

Box-control connection: much easier to operate and maintain

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

In addition to operating costs and attack efficiency, this packaging method also effectively reduces the operational and technical thresholds for threat actors. Novices only need to ensure that the configuration is correct, which means that threat actors can launch attacks with less understanding of "technical points", and the defender will face more and more sophisticated attackers.

1.3.2 Rental model-“Cloud Phone”

Optimization points: The rental model allows free "capacity expansion", which reduces the cost of maintaining equipment and facilitates the backup and transmission of device information. "Cloud Mobile" is an attack equipment rental model. The operator can directly operate the remote mobile phone (or virtual mobile phone) through the client or browser to launch attacks.

The trend of cloud mobile phones is the same as that of "group control" devices. More and more cloud mobile phones are packaged and sold with "one-click new phone", virtual positioning and agent IP. The price of such a packaged service is 4 yuan/day. Including the cost of receiving a phone number and the cost of the Internet, you can get a game ticket for just a few dozen to a hundred yuan. The cost is far lower than traditional attack methods on physical mobile phones. Enterprises face a more complex and broader reality of attacking people.

Experienced threat actors can also use cloud mobile phones to instantly "expand" their own attack device group when needed. The mode is really flexible.

Scenarios that were originally unable to be attacked due to the profit being lower than the cost of attack or the limit on the number of devices, can now be attacked due to the improvement of attack efficiency and flexible rental models. In the real environment, most studios basically attack certain companies in a certain industry while paying attention to marketing activities. At the right time, they use the idle residual value of the equipment to "piggyback" on some side businesses to make profits.



Operating page of a cloud-phone service

Source: Threat Hunter original report, page 41. Original image retained.

Pictured: A certain cloud mobile phone operation page

1.3.3 Central control

Optimization point: It solves the problem of limited number of devices in traditional group control caused by data lines transmitting screen data and command data.

The client is installed in the mobile device, and the user manages the mobile phone uniformly on the PC client and issues commands to it. After being transmitted over the network, the mobile client executes a simulated click to complete the attack.

1.3.4 Cloud Control

Optimization points: The devices do not need to be in the same location, and script commands are stored in the cloud. There is no need to send source code when trading scripts between groups, which facilitates script dissemination and management of a large number of mobile phones. A wide area network version of "central control" allows operators to manage mobile phones and issue commands through any browser.

1.3.5 Group Control

Optimization points: Early batch operation equipment solutions had many restrictions on script development. In order to avoid lags, the number of equipment was limited to about a hundred units.

The screen mapping method is used to map the mobile phone screen to the computer, and the mobile phone and the computer are connected through a hub through a data cable, thereby transmitting the screen content and operation instructions.

1.4 Attack and defense suggestions

Faced with the industrialized, professional, gang-oriented and chain-based operation model of today's threat actors, the offensive and defensive confrontation will be a protracted battle between enterprises and threat actors that continue to fight and grow.

Enterprises can fill cognitive blind spots, close information gaps, and understand the opponent's goals, attack ideas, and strategies through the comprehensive confrontation of anti-fraud intelligence (prevention beforehand, and finding protection points based on attack methods afterwards) + fraud data tags (locating attack traffic).

Familiar with the cost of the other party's crimes, and understand the resources, time, money costs, channel thresholds, upstream and downstream connections, and revenue obtained through the attack required by the other party to launch an attack. On the business side, comprehensively review your goals, compare the resources of both parties, adjust strategies, locate the attack accounts and traffic of threat actors, and attack and protect them.

threat actors win by quantity, but because of this, batches must have traces to follow. threat actors have a huge supply of upstream basic resources, but they are also very dependent on these resources. These are key nodes in the industrial chain, and they are also effective nodes for our identification, attack and protection. In the figure below, we provide suggestions on corresponding countermeasures that enterprise fraud controls can take against threat actors’ attack methods:

Threat-actor need	Solution or supporting industry	Key countermeasure
Batch attacks	Group-control devices	Group-control client detection; batch behaviour-trace detection; monitoring and analysis of attack tools; monitoring of at-risk interfaces
Large numbers of IPs not on blacklists	Rapid dial-up and mixed dial-up through soft-router home-broadband IP pools	New IP profiles with a time dimension
Large numbers of distinct device profiles	Software and hardware device-spoofing tools	Detection of device-spoofing tools
Receiving SMS and voice codes in bulk and sending unblock messages	Code-receiving platforms	Phone-number profiles
Passing human-verification checks	CAPTCHA-solving platforms	Monitoring of attack tools
Easy trading of basic resources	Account-sales platforms	Monitoring of account and resource costs and trading
Identity data (ID cards and numbers, bank cards and so on)	Data brokers	Monitoring and analysis of monetisation costs
Data trading, cash-out and money laundering	Trading of personal and company payment accounts; online laundering services; the dark web	Monitoring of dark-web trading

Threat-actor needs, solutions and key countermeasures

Source: Threat Hunter original report, page 43. Table re-typeset in English from the original.

- Anti-fraud intelligence - the hidden power in business security attack and defense. The intelligence deployed and collected from the upstream and downstream perspectives of the entire industry chain can be used as an explanation and support for fraud-control strategies. At the same time, fraud intelligence such as threat actors' public opinions and trends can also effectively feedback the effectiveness of corporate fraud-control strategies and help companies control offensive and defensive costs.

Anti-fraud intelligence generally includes: the interface that threat actors prepare to attack, the trading platform involved, the target interface of the attack, the attack tools used, the related resources involved (phone number, IP), etc. Through the deployment and control of these nodes, risks can be effectively discovered in time when threat-actor resources are prepared, and the attack paths and logic of threat actors can be understood, and fraud-control strategies can be prepared in advance.

- Fraudulent data labeling - an efficient identification solution. No matter how the threat actors iterate in terms of technology and equipment, they can't always bypass some basic fraud resource reserves when launching attacks, such as the phone number used for registration and the accessed IP. According to our statistics, there are 8 million malicious registration attacks launched by threat actors on the entire network every day, and more than 1.5 million active fraudulent phone numbers are active every day, with an average of 6 attacks per phone number per day. If the basic resources used by threat actors are monitored from the perspective of threat actors and the fraudulent resources of threat actors in corporate business scenarios are identified, these cybercrime ecosystem fake accounts that conduct malicious activity can be directly intercepted or demoted. The fraud controls method based on the basic resource identification of threat actors can reduce the misjudgment rate of fraud controls to a certain extent and improve the interpretability.

2. Evolutionary history of threat actors IP resources

IP, as the most basic identity in the Internet space, has always been the most intense point of attack and defense between threat actors and Party A.

However, after Threat Hunter has been deeply involved in the field of business security for several years, it has been discovered that the speed of iterative evolution of threat actors technology is staggering. However, many parties' research and understanding of threat actors are still at the primary stage in the early years. threat actors are developing rapidly, but Party A's understanding of threat actors has stagnated, which will inevitably lead to information mismatch in the attack and defense process, increased defense difficulty, delayed defensive response, and greatly reduced efficiency and effectiveness.

For example, for threat actors, "second dial" is no longer a new word. Second dial IP resources have already become the mainstream IP resources for threat actors. However, in the process of communicating with multiple Party A customers, Threat Hunter found that many students who work in Party A's business security have little or no understanding of the concept of second dial.

This phenomenon is worth reflecting on. Speed dialing was already a mature IP resource solution around 2014. As of 2019, it has been widely used in risk scenarios that require a large amount of IP resources in a short period of time, such as batch registration, voting, and volume traffic manipulation. Moreover, due to the difficulty of identifying speed dial IP, it has caused great harm to the current Internet business security scenario. However, many students in the security industry actually think this thing is very new.

Whether it is the confrontation point of IP, or other confrontation points such as phone numbers, device fingerprints, risky traffic and behaviors, the traditional passive confrontation method of "first being attacked", then "discovering afterwards", and finally "supplementary rules" is completely unable to adapt to the current rhythm of attack and defense with threat actors. Only by studying threat actors, understanding threat actors, and mastering the latest technologies and trends of threat actors can we control more initiative.

If you want to win the war on business security, you must transform from a "repairing the situation" type of offense and defense to a "preparing for a rainy day" type of offense and defense.

2.1 second dial

Since Party A began to implement fraud controls at the IP level based on some simple rules (such as setting thresholds for the number of IP visits per unit time, limiting IPs that trigger specific behaviors, etc.), it has officially declared war on threat actors on the IP battlefield.

In the early days, threat actors mainly used proxy IPs to bypass Party A's fraud-control rules, and websites selling proxy IPs sprung up like mushrooms after a rain. The way these websites collect proxy IPs mainly uses high-performance servers to scan the entire network, scan servers that open proxy services, or directly crawl data from other proxy websites, collect valid proxy IPs and ports, and deliver them to users for free or for a fee. The biggest disadvantage of this method is that the effectiveness and number of proxy IPs cannot be controlled, the proxy website cannot be controlled, and users cannot control it, which greatly affects the efficiency of threat actors in automated attacks. There are also threat actors who use VPN to bypass

For customer fraud controls, VPN is relatively stable, but it is more expensive and has a limited number of valid IPs, which is not suitable for large-scale batch attacks by threat actors.

The number of proxy IPs in the entire network is relatively limited, and early proxy services were generally installed on servers in data centers. Many parties gradually began to accumulate proxy IP pools, further suppressing the effect of threat actors using proxy IPs.

Many students who are engaged in business security only have this understanding of threat actors IP resources. However, the unwilling threat actors began to upgrade resources and developed the technology of instant dialing.

In layman's terms, the underlying idea of second dial is to use the principle of domestic home broadband dial-up Internet access (PPPoE), and a new IP will be obtained every time the connection is disconnected and reconnected. threat actors who keep pace with the times master a large number of broadband line resources, use virtualization and cloud computing technologies to package them into cloud services, and use ROS (soft routing) to uniformly deploy and manage virtual hosts and broadband resources. This kind of cloud service delivered to users of threat actors is actually a cloud host (commonly known as "second dial machine"). Users of threat actors can install desktop or Linux operating systems, connect through RDP, VNC or SSH, and deploy tools to automatically disconnect, reconnect, switch IP and attack, and then launch attacks.

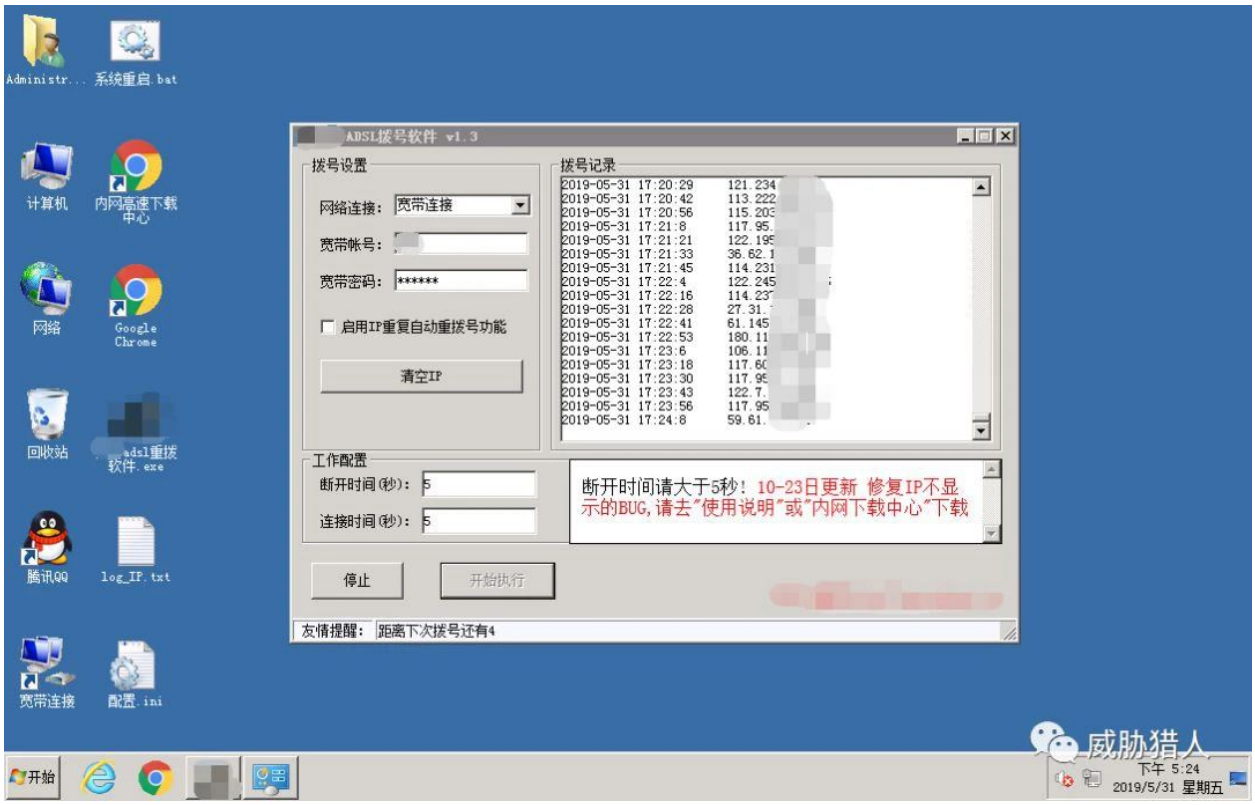
Screenshot of the web management page of the instant dialer:



Web management page of a rapid dial-up server

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

Screenshots of the dial-up desktop and a certain dial-up software (threat actors users can switch IPs in seconds):



Rapid dial-up desktop and dial-up software switching IPs in seconds

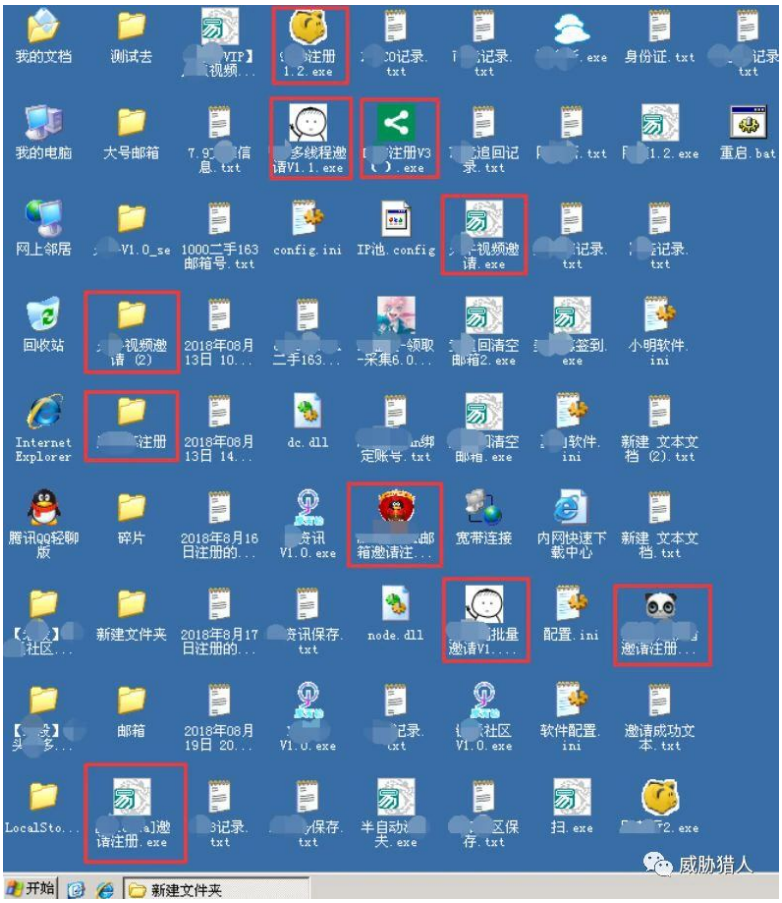
Source: Threat Hunter original report, page 46. Original image retained.

As mentioned above, the underlying idea of dial-up is to use the principle of domestic home broadband dial-up Internet access (PPPoE), and a new IP will be obtained every time the connection is disconnected and reconnected. This gives MiDial two natural advantages in terms of confrontation with Party A's IP strategy:

- Huge IP pool: Assume that the broadband resources on a certain second wave machine belong to the telecom operators in the XX area, then the second dial machine can dial the IPs in the entire telecom IP pool in the XX area, ranging from a hundred thousand to a million;
- Difficult to identify Second Dial IPs: Because Second Dial IPs and normal user IPs are taken from the same IP pool, there is a high probability that the Second Dial IPs will be transferred to normal users after their usage period (usually at the second or minute level) ends, so it is very difficult to distinguish Second Dial IPs from normal user IPs.

These two natural advantages are also the core reasons why dial-up is the current mainstream IP resource for threat actors.

A large number of registration machines and other threat-actor tools and resources were found on a dial machine:



Registration bots and other tools found on one rapid dial-up machine

Source: Threat Hunter original report, page 47. Original image retained.

In addition, threat actors have also upgraded the speed dial, which is called "hybrid dialing". That is, threat actors have opened up the speed dial resources of multiple provinces, cities and regions, so that a single speed dial machine can dial the IP resources of hundreds of regions across the country. The cost of a mixed dialing machine is as low as 48 yuan/month.

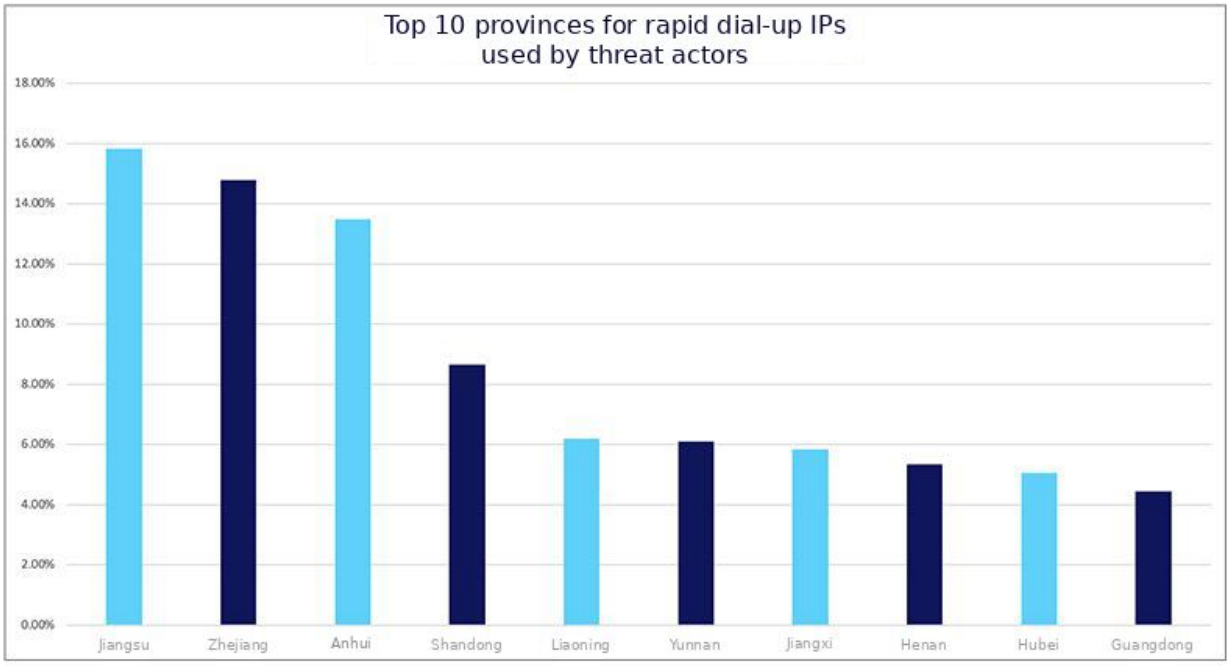
Threat Hunter has made statistics on the mainstream platforms that provide instant dialing machines on the market. The instant dialing IP provided by Threat Hunter can cover all about 300 cities in the country.



Rapid dial-up IP resources cover the whole country

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

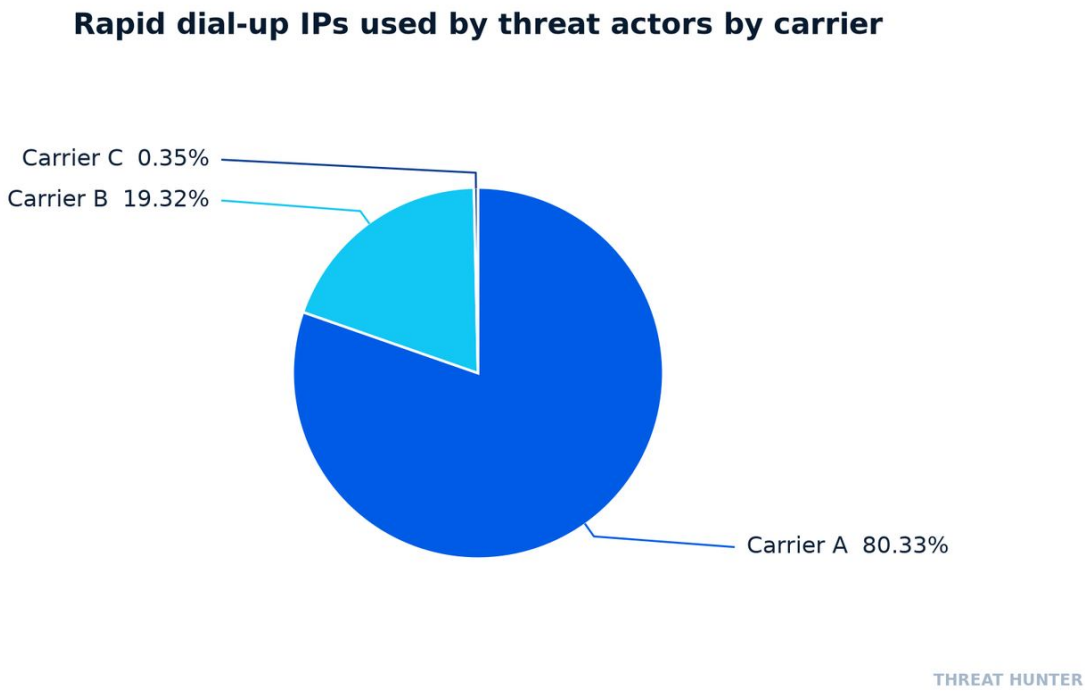
The top ten provinces with threat actors instant dial IP resource distribution are:



Top 10 provinces for rapid dial-up IPs used by threat actors

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

In addition, the proportion of threat actors' instant dial IP resource operators are:

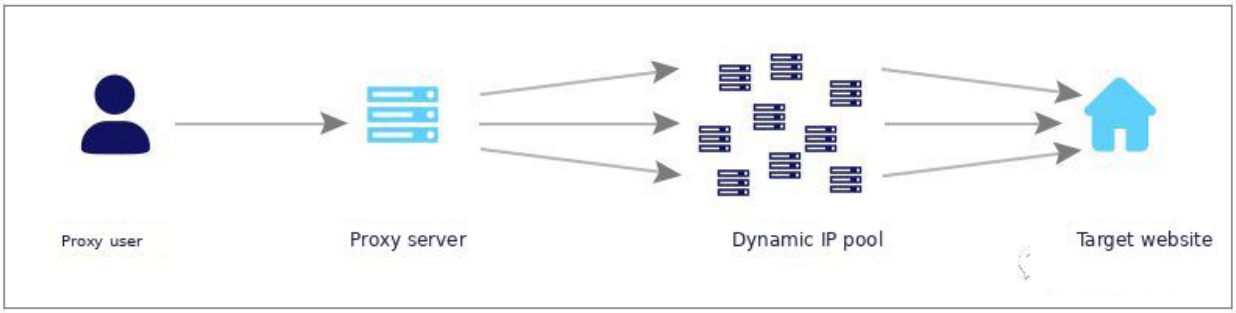


Rapid dial-up IPs used by threat actors by carrier

Source: Threat Hunter original report, page 49. Redrawn in English from the original figure.

threat actors is also constantly expanding the geographical coverage of its dial-up IP resources, and some platforms can even provide the United States and South Korea. Hong Kong and other non-mainland IP resources.

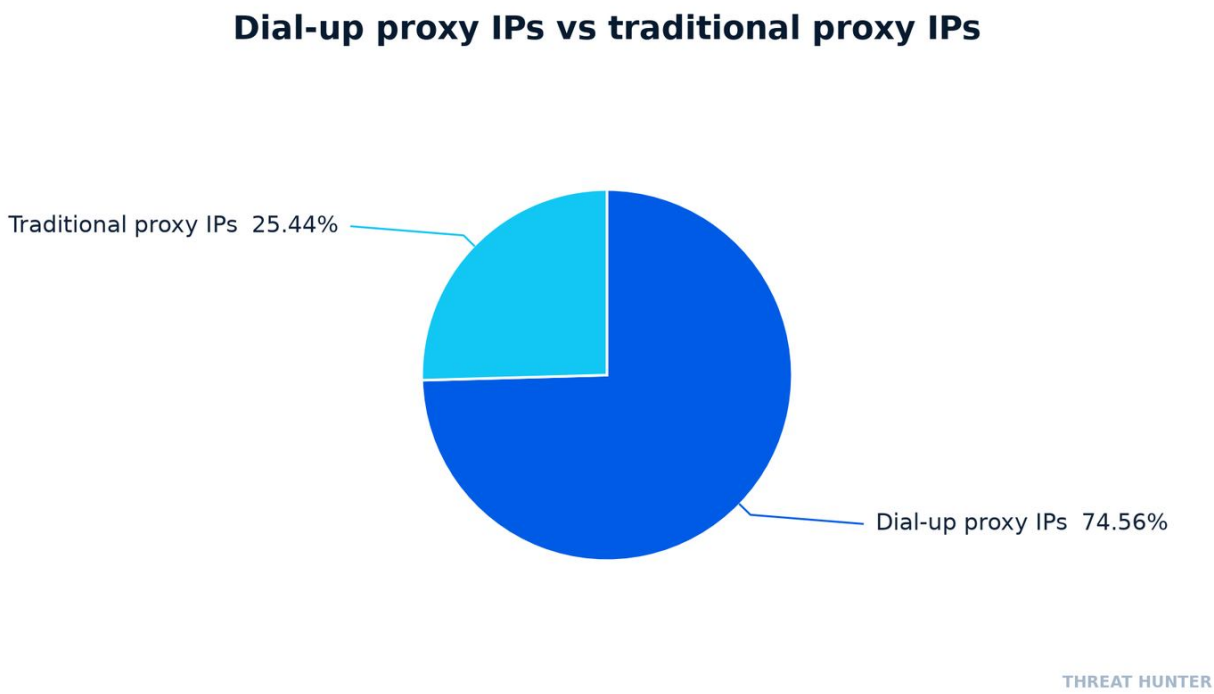
In addition, as mentioned in the previous article, the early method for threat actors to collect proxy IPs was to scan the entire network, and availability could not be guaranteed. In fact, threat actors have already applied the speed dial technology to proxy IPs. threat actors use the speed dial technology to accumulate proxy IP pools and then provide them to downstream threat actors users. Moreover, this type of proxy IP inherits the advantages of speed dial IP. First, the IP pool is huge, and second, it is difficult to identify. A common implementation method for dial-up proxy IP is dynamic forwarding, as shown in the following figure:



How a dial-up proxy forwards traffic dynamically

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

Data from the Threat Hunter intelligence monitoring platform shows that among the proxy IP resources currently used by threat actors, instant dial proxy IPs account for 74.56%, while traditional proxy IPs account for only 25.44%. If Party A still wants to confront threat actors in the traditional way of accumulating IP pools, it will inevitably introduce a large number of false positives.



Dial-up proxy IPs vs traditional proxy IPs

Source: Threat Hunter original report, page 50. Redrawn in English from the original figure.

In addition, using the desktop, Android or iOS client provided by the proxy platform, through VPN protocols such as PPTP/LT2P, threat actors' terminals can be directly turned into "second dialers", which greatly improves the convenience of threat actors' malicious activity deeds.

2.2 Attack and defense suggestions

In short, instant dialing has become the core technology that supports threat actors and Party A's IP-level attack and defense, and is also one of the pain points in the current business security industry. The article mentioned that the two natural advantages of instant dialing are two natural barriers for threat actors, but they bring great difficulty to Party A in identifying and judging risky IP.

Under the current situation, the confrontation with threat actors at the IP level relies on the traditional method of accumulating IP threat intelligence libraries, which cannot be directly applied and implemented on the business side. The typical use effect is that the detection rate of black IPs is very high, and the misjudgment rate of normal user IPs is also very high.

Therefore, the core basis for identifying risky IP should be whether the IP is currently held by threat actors. The two indicators of the IP's threat actors usage cycle and time validity are particularly important, especially for "non-shared" IP such as home broadband IP and data center host IP. For "shared" IPs such as base stations and dedicated exits, since there will be a large number of users behind a single IP, the fraud-control threshold should be relatively loose. However, if it can be accurately identified whether the IP is currently being used by threat actors, it can also provide important reference value.

Threat Hunter has long been committed to the research of threat actors IP resources, aiming to help Party A solve the problem of identifying risky IPs in business security scenarios, and has recently achieved a breakthrough. By deploying and controlling threat actors' ROS dial-up nodes, it

can monitor and collect the dial-up IP currently used by threat actors in real time. Threat Hunter is willing to work together with all parties to communicate and work together to overcome industry technical problems.

3. Case Analysis of Second-Dial IP Identification Technology

IP is the most basic identity of the Internet and an indispensable underlying resource support for the development of the cybercrime ecosystem. If IPv4 is a planet, then IPv6 is an entire universe, and its address space is nearly infinite.

The IP we currently refer to usually refers to the IPv4 address, which is also one of the most intense attack and defense points in our current security confrontation with threat actors.

IPv4 consists of 32 binary bits, and there are 2^32 (about 4.3 billion) addresses in the space, of which about 280 million addresses are reserved for special purposes. However, as addresses continue to be allocated to end users, the problem of IPv4 address exhaustion is also arising.

This situation has stimulated the advancement of IPv6 as the current only long-term solution.

Compared with IPv4, IPv6 consists of 128 binary bits and has 2^128 (approximately 3.4×10^38) addresses. It is IPv4’s

7.9×10^28 times, the huge address space is almost infinite, and it is very vividly said that it can provide every grain of sand in the world.

The child is assigned an address.

However, as a blessing and a curse, the address space of IPv6 far exceeds the current IPv4, which also means that the amount of IP resources controlled by cybercriminal groups will also expand infinitely, and they will be able to use an IP independently for each malicious account. The fraud-control strategies accumulated in the past confrontation process and the complete IPv4 security system will face new challenges after the large-scale popularization of IPv6.

In network development, security comes first. The data monitored by Threat Hunter Guigu Lab shows that there is already malicious machine traffic initiated on the IPv6 address of the data center, and IPv6 proxy resources have already appeared in foreign cybercrime markets. The laboratory speculates that this is related to the popularity of IPv6 to a certain extent. As domestic IPv6 deployment gradually unfolds, cybercriminal attacks based on this will inevitably follow the trend. It is worth noting that the IP resource of threat actors that currently causes the most headaches for business parties - Mingdial, has also quietly added support for IPv6.

3.1 cybercriminal groups have begun to utilize IPv6 resources

The development of IP resources driven by strong market demand has become an important link in the cybercrime ecosystem chain, and cybercriminal groups that specialize in providing IP resources have also emerged.

The technology of cybercriminal groups are very advanced with the times, and the attack methods have also been upgraded in the process of playing "cat and mouse game" with enterprises. For example, from the early method of bypassing fraud-control rules through proxy IP, now it has

evolved into "second dial" and "mixed dial". Party A's countermeasures have also been improved and accumulated accordingly in the IPv4 environment.

However, when IPv4 begins to migrate to IPv6, changes in the IP environment not only involve corresponding changes in network equipment, routing management, and IPv6 protocol stacks, but the fraud-control system built under IPv4 will also face transformation and upgrades during the migration process.

If the protection strategy originally applicable to IPv4 is not transformed in time, how much risk will it face? This is a question that all enterprises need to consider and face. For example:

- Massive address scanning: IPv6 is composed of 128 binaries, which means that if a subnet uses 64 bits in the IPv6 network to allocate IP, the total capacity of the subnet, that is, the number of assignable IPs is 2 to the 64th power. Assume that traversing all IPv4 addresses takes an hour. Then it would take 500,000 years to traverse all the IP addresses under this subnet...
- Blacklist database failure: The large amount of black IP data accumulated in the IPv4 environment is significantly helpful in identifying threat actor IPs. However, when the IPv6 era comes, nearly unlimited IP addresses will have a strong impact on the blacklist database. The originally efficient identification mechanism will be close to "ineffective" in the IPv6 environment.
- Misjudgment under the unknown: In the initial stage of IPv6 deployment, there will be problems such as missing risk data such as IPv6 geographical location and device fingerprints, which will lead to the inability to accurately determine the nature of IP and lead to misjudgment.
- ...

At present, the global IPv6 penetration rate reaches 23.97%, the IPv6 penetration rate in developed countries is 25%, and the IPv6 penetration rate in Asia reaches

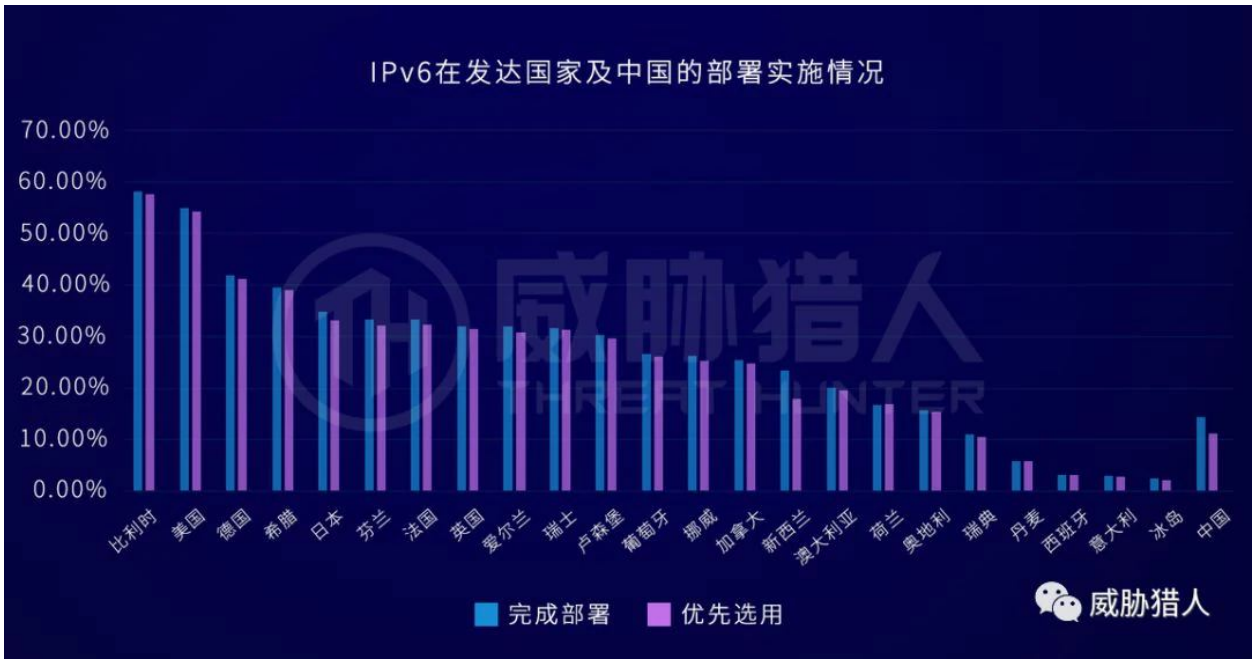
27. 13%, among which China’s IPv6 penetration rate reached 14.46%. The following is IPv6 in various continents and developed countries, as well as China

Popularity statistics:

Code	Region	IPv6 capable (%)	IPv6 preferred (%)	Samples
XA	World	23.97	23.09	293,846,120
XC	Americas	31.03	30.47	52,828,771
XD	Asia	27.13	25.86	167,014,860
XF	Oceania	18.37	17.34	2,077,224
XE	Europe	18.01	17.70	43,239,026
XB	Africa	1.93	1.87	28,679,767
XG	Other	14.26	14.25	110,284

IPv6 adoption by continent

Source: Threat Hunter original report, page 53. Table re-typeset in English from the original.



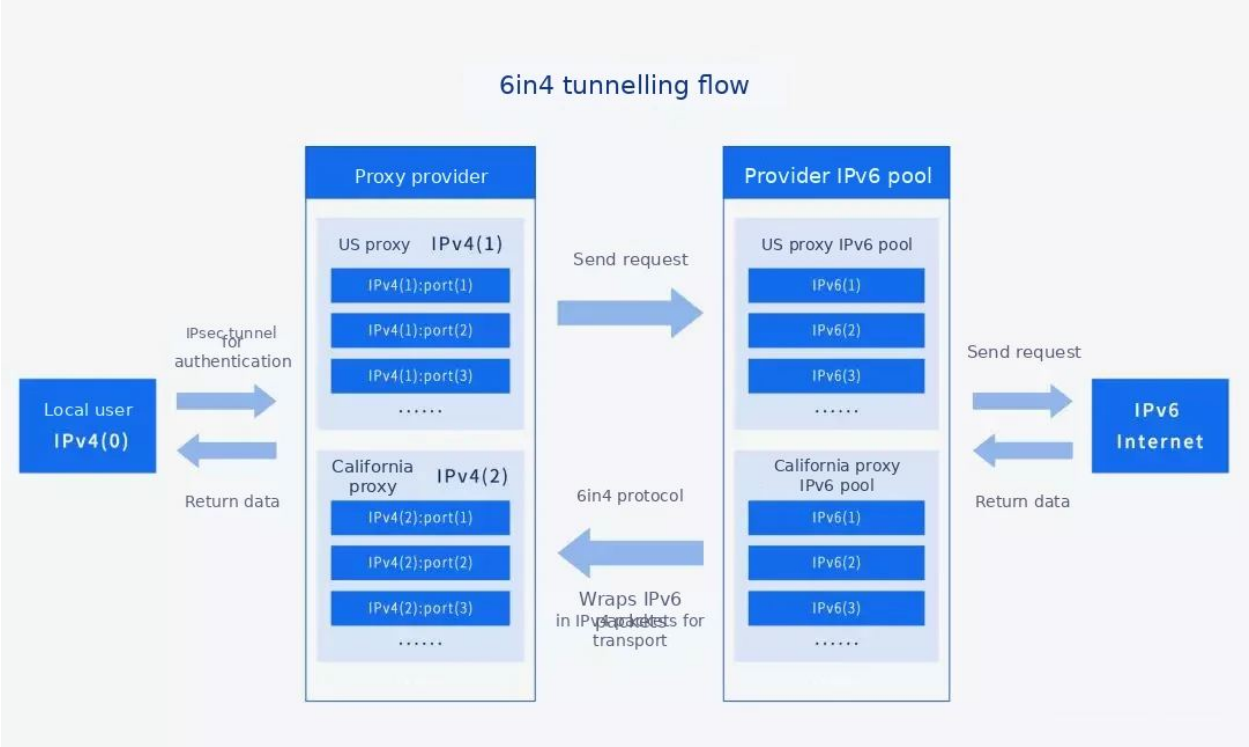
IPv6 deployment in developed countries and China

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

Subsequently, we checked the malicious machine traffic captured by the Threat Hunter monitoring platform. By analyzing the resources, we found that there are traces of IPv6 in the main IP resources currently controlled by cybercrime ecosystem.

1)Agent

According to surveys, foreign proxy platforms have already sold IPv6 proxies. Since the current IPv6 penetration rate is still low, IPv6 agents do not directly provide IPv6 addresses and ports. They still provide IPv4 and ports. IPv6 data packets are encapsulated in IPv4 data packets through a tunnel protocol similar to 6in4 plus IPsec.



How 6in4 tunnelling delivers IPv6 proxies over IPv4

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

We collected these IPv6 proxies, analyzed their characteristics, and found that they mainly come from foreign IDC computer rooms.



An IPv6 proxy offered by a proxy platform outside China

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

Compared with foreign countries, there is no domestic platform that specializes in selling IPv6 proxies in bulk, but we have also captured some domestic IPv6 proxy samples. What is interesting is that most of the domestic IPv6 proxies originate from the IDC computer room of the domestic education network.

Due to the nature of the education network, if the IPv6 segments corresponding to the IDC of each education network are simply intercepted, the most direct result will be to accidentally injure a large number of normal student users.

2) Second-dial Second-dial IP is another major IP resource controlled by cybercrime ecosystem, and some speed-dial companies have now begun to support and provide IPv6 services.

We analyzed the IPv6 address obtained from the dial-up machine and found that its nature belongs to domestic home broadband. Using the principle of dial-up Internet access (PPPoE), a new IP will be obtained every time the connection is disconnected and reconnected. It is similar to IPv4's instant dialing properties, but has an advantage over IPv4 in that its IP pool is so huge that it is nearly infinite, and the IP address is more difficult to identify.

- Unlimited IP pool Assume that the broadband resource on a certain dial-up phone belongs to a telecom operator in the XX area. Then the dial-up phone can dial the IPs in the entire telecom IP pool in the XX area, which can range from hundreds of thousands to millions in an IPv4 environment. In the IPv6 environment, the magnitude is huge and difficult to estimate. We conducted repetitive statistics on a certain batch of IPv6 addresses and found that there were almost no duplicate IPv6 addresses among the 100,000 monitored data, but the number in the actual IPv6 dial pool was far more than this number. This means that the traditional method of using IP blacklists to label IP risks will no longer be applicable.
- Second dial IPs are difficult to identify. In addition, because second dial IPs and normal user IPs exist in the same IP pool, every time the connection is disconnected, the second dial IPs originally used by threat actors may flow into the hands of normal users during the next dial-up. This will make it very difficult to distinguish between second dial IPs and normal IPs.

3.2 Attack and defense suggestions

In the development of the next generation Internet based on IPv6, the seemingly inexhaustible IP resources have indeed brought salvation to the current gradually depleting IPv4, but it is also the hidden security risks behind the "inexhaustible" that cannot be ignored. From the above data, we can infer that the utilization of IPv6 by cybercriminal groups are largely related to its popularity.

Since the popularity and adoption of IPv6 are at a high level in most developed countries, platforms that specialize in selling IPv6 agents have also been born. At present, when most mainstream websites in China do not yet support IPv6 access, cybercriminal groups have begun to study IPv6 technology and utilize IPv6 resources. When the scale of IPv6 deployment in China follows the step-by-step implementation and advancement of policies, IPv4 has to shift to IPv6. If the transformation and upgrading of enterprise fraud controls facilities do not keep up with the pace of deployment, there will be a period of "empty window" for security protection. cybercriminal groups can effortlessly enter the platform, make waves, and sing and dance.

Therefore, taking precautions is the best way for enterprises to deal with risks. We have reason to believe that when more and more domestic websites support IPv6, and the functionality and stability tend to be improved, the IPv4-based offensive and defensive battlefield will inevitably shift to IPv6. For all

While ensuring the stable upgrading of technology, it is equally important to consider security issues. As a pioneer in the business security industry, Threat Hunter has invested a lot of manpower and resources in the research of IPv6 threat-actor resources, and has begun to accumulate real-time IPv6 risk data, hoping to help companies migrating to IPv6 solve unexpected security issues.

4. Case analysis of the new tool “IP Magic Box”

As we all know, IP resources are the core resource for threat actors to carry out large-scale attacks. Threat Hunter's past reports have discussed extensively that threat actors use proxy IP, dial-up IP and other technologies to bypass IP detection to carry out attacks.

According to Threat Hunter's long-term research, it is known that this type of IP is essentially home broadband, data center and other IP. Through certain technical means, IP and equipment can be associated and tagged within a certain period of time.

However, as the offensive and defensive confrontation escalates, threat actors shift their attention to the more hidden base station IP. Recently, Threat Hunter discovered a tool that allows PC devices to use base station IP. threat actors call it the "IP Magic Box."

4.1 IP Magic Box

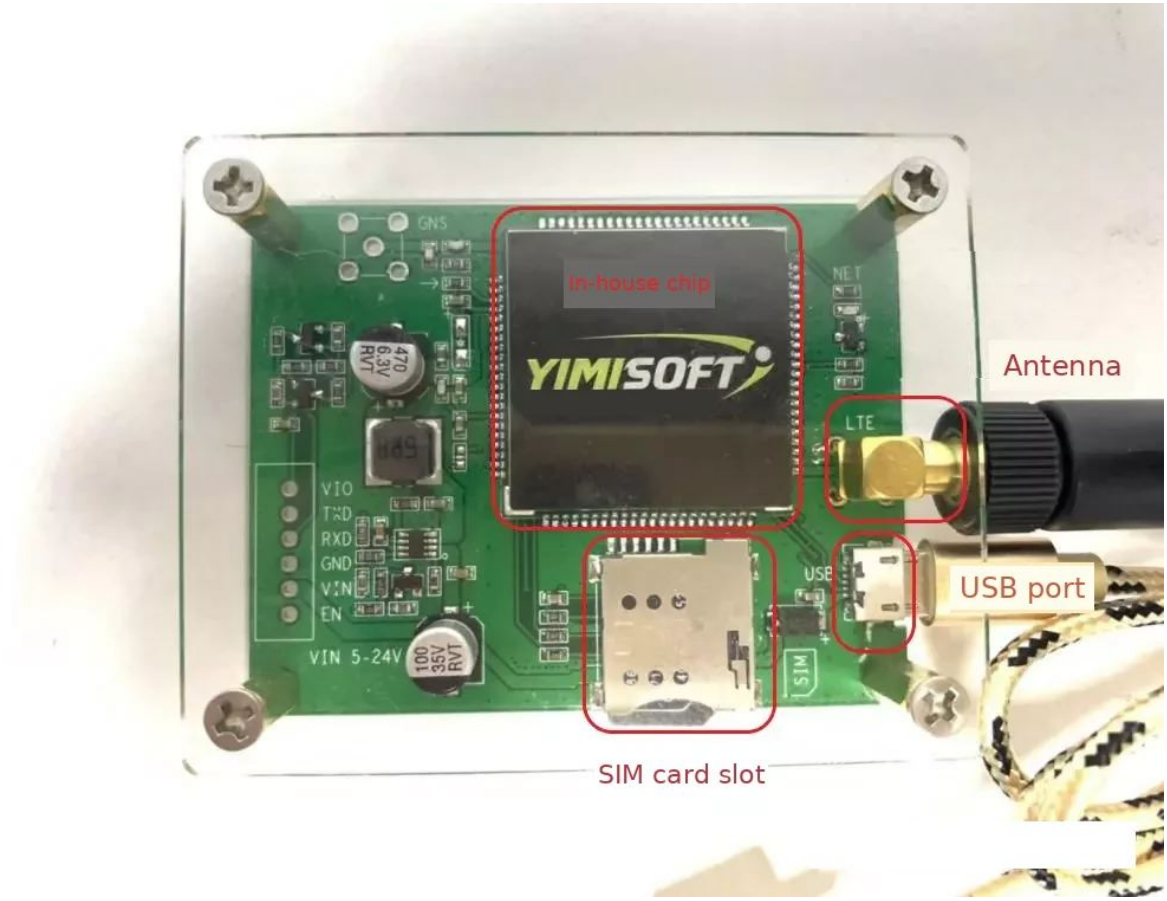
IP Magic Box is a hardware box smaller than the palm of your hand. After USB connection, it can make ordinary PC have base station IP.

Its motherboard design is simple and easy to use. It is not only compatible with domestic SIM cards of China Telecom, China Mobile and China Unicom, but also supports SIM cards issued outside mainland China. It connects to the personal host through the USB interface of the self-developed chip module set, allowing the PC to achieve 4G Internet access. Then download the script to simulate switching flight mode and install the corresponding driver, and then you can switch the IP.



IP Magic Box device

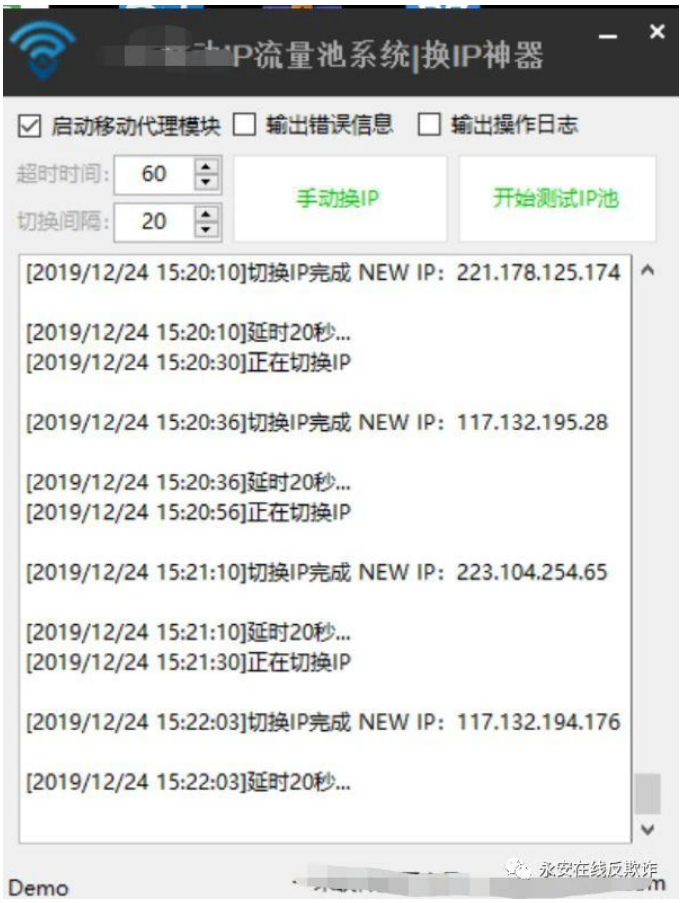
Source: Threat Hunter original report, page 57. Original image retained.



IP Magic Box board: antenna, USB port and SIM card slot

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

Pictured: IP Magic Box Equipment Pictured: IP Magic Box Chip



IP Magic Box control software on a PC

Source: Threat Hunter original report, page 58. Original image retained.

Pictured: The IP Magic Box control terminal on a PC. The IoT card used in conjunction with the IP Magic Box is even more affordable and easy to use.

We summarized that the IP magic box has the following characteristics:

1) Many associated users: A base station IP will be associated with a large number of user groups. If the IP is intercepted, it is easy to accidentally kill normal users, affect the user experience, and lead to user loss.

2) Switching IP is simple: you only need to turn on and off airplane mode to achieve IP switching.

3) Lower cost: According to our statistics, the general national IoT card opening price is 4-6 yuan, and the price of 10G traffic is only 15 yuan.

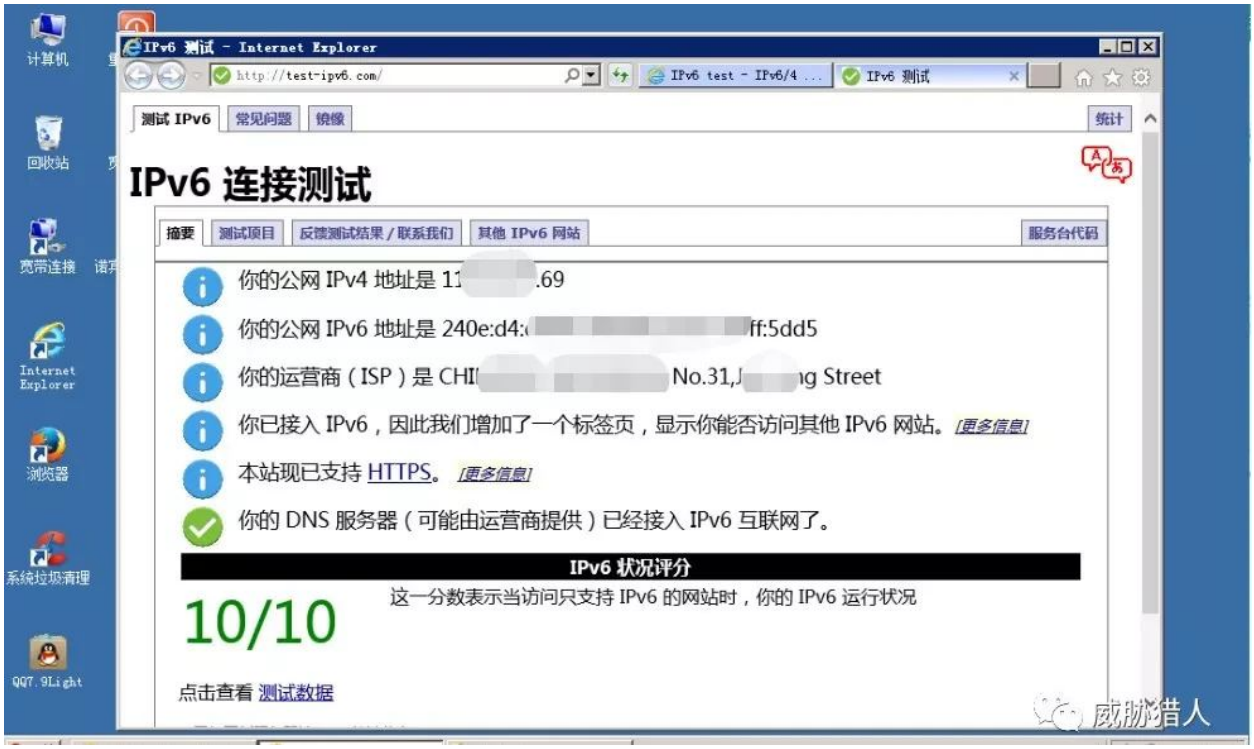
4) Massive IP pool: After testing, a national IoT card can obtain at least 17 IP segments, which are distributed in different regions.

Because of the special way IP Magic Box obtains IP, it is much better than dial-up IP and proxy IP in all aspects of IP volume, attack efficiency, price cost, detection method, and deployment cost. The following table shows the comparison results:

	IP Magic Box	Rapid dial-up IP	Proxy IP
IP volume	Uses real mobile-carrier IPs; can switch to any IP within a short time	Huge pool of home-broadband IPs; how many IPs can be switched in a short time depends on the size of the soft router's IP pool	Limited: one provider's pool is usually 10,000 to 20,000 IPs
Attack efficiency	Uses 4G: stable network, high bandwidth	Used through VPS; bandwidth and machines become unstable as users increase	Very unstable: most proxy providers get IPs by scanning and crawling; IPs stay valid for about 5 minutes
Cost	Hardware box: 900 yuan; IoT card: 4–6 yuan each; data: 10 GB for 8–15 yuan a month	2 Mbps bandwidth: 50–200 yuan a month	10,000 IPs: 100 yuan a month
Detection	Real carrier base-station IPs shared by many real users; risky IPs can only be flagged	Risky IPs can be flagged and blocked over a short time window	Few IPs; easy to detect by clustering
Deployment	Install a script and driver; toggle airplane mode for a new IP	Log in to the VPS to operate; limited by VPS performance	Integrate in code through the API

IP Magic Box vs rapid dial-up IPs vs proxy IPs

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



Testing IPv6 support over rapid dial-up

Source: Threat Hunter original report, page 59. Original image retained.

Pictured: Using seconds dial to test IPv6 support. The laboratory tested various mainstream domestic websites through IPv6 and found that most companies have not started to support IPv6 access. A small number of companies that support IPv6 only support the main network to be accessed through IPv6, but the loading speed of web pages and the stability of access links are somewhat unsatisfactory. Once user login or other user operations are required, access failures or login timeouts often occur. However, foreign websites that support IPv6 access are much better

than the domestic situation in terms of stability, response rate, and support for user-related operations.

5. Customized ROM modification case analysis

Machine modification is an important technical means that threat actors rely on to commit large-scale malicious activity. By modifying the machine, threat actors can forge new equipment in batches, thereby bypassing Party A's business fraud controls. Therefore, the attack and defense around modified aircraft is one of the key research tasks in our fight against the cybercrime ecosystem. In the past few years, the methods used by threat actors to modify their phones have mainly included Android emulators, modification tools, and application multi-openers/clones.

Through the Karma business intelligence monitoring platform, we found that cybercriminal groups began to use a new method last year, that is, customized ROM to modify the machine. This modification technology is lower-level and more difficult to detect. The current technology is becoming more and more mature.

After a period of in-depth research, we upgraded the device risk SDK some time ago to fully support the detection of customized ROM modified machines.

5.1 Technical principles of custom ROM modification

To put it simply, by modifying the Android system source code, the device parameters are directly modified and returned at the bottom layer. This modification is global, that is, it can take effect on all application processes and shell processes.

5.1.1 Modify model information

Let's take modifying model information as an example. Obtaining model information will mostly call the _system_property_get function, which is located in the system library /system/lib/libc.so. On the device that customizes the ROM machine, the function code is as follows:




```
int __fastcall __system_property_get(int a1, _BYTE *a2)
{
  _BYTE *buffer1; // r4
  const char *key; // r5
  int result; // r0
  _DWORD *v5; // r0

  buffer1 = a2;
  key = (const char *)a1;
  if ( !shouldGjInLibc() )
    goto LABEL_15;
  if ( !j_strcmp((int)"init.svc.mtpd", (int)key) )
  {
LABEL_11:
    result = 0;
    *buffer1 = 0;
    return result;
  }
  if ( !j_strcmp((int)"sys.usb.config", (int)key) || !j_strcmp((int)"sys.usb.state", (int)key) )
  {
    buffer1[2] = 112;
    *(_WORD *)buffer1 = 29805;
    buffer1[3] = 0;
    return 3;
  }
  if ( j_strcmp((int)"persist.sys.usb.config", (int)key) )
  {
LABEL_15:
    if ( isWgProp((int)key) )
      return wgzs_property_get(key, buffer1);
    v5 = (_DWORD *)j___system_property_find(key);
    if ( v5 )
      return j_j___system_property_read(v5, 0, (int)buffer1);
    goto LABEL_11;
  }
  *(_DWORD *)buffer1 = 0x656E6F6E;
  buffer1[4] = 0;
  return 4;
}
```

Custom ROM code that spoofs device-model information

Source: Threat Hunter original report, page 60. Original image retained.

You can see that the developer of the custom ROM has modified the function and added his own code logic. If a certain attribute is customized in the machine modification tool, the attribute value will not be obtained through the system's default reading function, but the tool's customized reading function will be executed. At the same time, we found that the developer had deeply customized the init process, and finally modified the model information in init.

5.1.2 Modify IMEI

Obtaining IMEI information usually calls the getDeviceID function. This is an IPC call for the phone service. The response code is located in: packages/services/Telephony/src/com/android/phone/PhoneInterfaceManager.java, as shown below:




```
3166        ImsManager.setVtSetting(this.mPhone.getContext(), enable);
        }

3170    public boolean isVideoCallingEnabled(String callingPackage) {
3171        if (canReadPhoneState(callingPackage, "isVideoCallingEnabled") && ImsManager.isVtEnabledByPlatform(this.mPhone.getContext(
3181            return ImsManager.isVtEnabledByUser(this.mPhone.getContext());
            }
3171        return false;
        }

3185    public boolean canChangeDtmfToneLength() {
3186        return this.mApp.getCarrierConfig().getBoolean("dtmf_type_enabled_bool");
        }

3190    public boolean isWorldPhone() {
3191        return this.mApp.getCarrierConfig().getBoolean("world_phone_bool");
        }

3195    public boolean isTtyModeSupported() {
3197        return TelecomManager.from(this.mPhone.getContext()).isTtySupported();
        }

3201    public boolean isHearingAidCompatibilitySupported() {
3202        return this.mPhone.getContext().getResources().getBoolean(R.bool.hac_enabled);
        }

3214    public String getDeviceId(String callingPackage) {
            Phone phone;
3215        if ("com.kexunjie.gj.forsystem".concat("_cache").equals(callingPackage)) {
3216            return WgzsUtil.getOrgHwFlags();
            }
3218        if (canReadPhoneState(callingPackage, "getDeviceId") && (phone = PhoneFactory.getPhone(0)) != null) {
3224            return phone.getDeviceId();
            }
3215        return null;
        }
```

Custom ROM code returning the IMEI

Source: Threat Hunter original report, page 61. Original image retained.

You can see that the IMEI value is returned, and the phone.getDeviceId function is called. Further follow up its code, as shown below:




```
public String getDeviceId() {
    String mImei2 = this.mImei;
    if (WgzsUtil.shouldGJInService(Binder.getCallingUid())) {
        Log.d("PhoneHook", "call getDeviceId and should gj");
        return getHookValue("IMEI");
    } else if (isPhoneTypeGsm() || ((CarrierConfigManager) this.mContext.getSystemService("carrier_config")).getConfigForSubId(getSubId()).getBoolean("force_imei_bool")) {
        return mImei2;
    } else {
        String id = getMeid();
        if (id != null && !id.matches("^0*$")) {
            return id;
        }
        loge("getDeviceId(): MEID is not initialized use ESN");
        return getEsn();
    }
}
```

Custom ROM code that swaps in a forged IMEI

Source: Threat Hunter original report, page 61. Original image retained.

It can be seen that based on the UID of the IPC call initiator (which can be regarded as a unique identifier), it is determined whether the IMEI needs to be modified. If so, calling getHookValue returns the fake IMEI. For ease of use, the author provides a setting interface to set which applications need to modify the IMEI before use.

5.2 Use of customized ROM modification machine

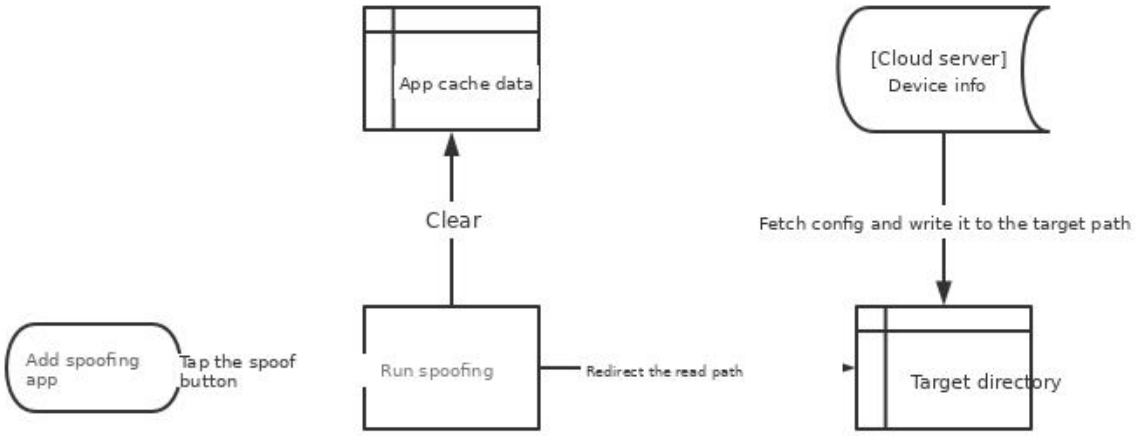
Since custom ROM modification directly modifies the Android source code, the object of modification is a real device, and there is no intrusion into the application itself, so it is difficult to detect, and the modification effect is very stable. In addition, the use of customized ROM modification machine is also very convenient:

1) The data environment of the model can be mirrored and backed up to the cloud server to facilitate the management of the device environment corresponding to the account;

2) Open up the system debugging interface to facilitate automated script writing and reduce development costs;

3) Fool-style one-click operation to complete device information modification and device data recovery.

The operation process of custom ROM modification is shown in the figure below:



How custom ROM device spoofing works

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

Based on the intelligence data of the Karma business intelligence monitoring platform, traffic diversion is one of the main usage scenarios of customized ROMs. Practitioners of threat actors can easily realize the reuse of equipment by customizing ROM modifications, and then combine it with customized scripts to perform batch and automated traffic diversion operations.



Phones running a custom ROM for traffic diversion

Source: Threat Hunter original report, page 63. Original image retained.

5.3 Detection of customized ROM modification machine

Detecting the offensive and defensive planes of other modification technologies is difficult to apply to customized ROM modifications. Therefore, it is necessary to find new attack and defense planes based on in-depth analysis of customized ROM modification tools and combined with the actual operating principles and operating processes of the tools. At present, for several active custom ROM modification tools, we have found attack and defense planes that are difficult for the tools to counteract, and have defined detection logic for each tool on top of them. Our device risk SDK was also upgraded as soon as possible.

Of course, attacking and defending against threat actors is always a process of continuous confrontation. If you only rely on the same defense mechanism, it will eventually be cracked one day. Especially at most times, the defender will be more passive than the attacker, so it is necessary to establish a closed loop from problem discovery to quick solution to minimize business losses.

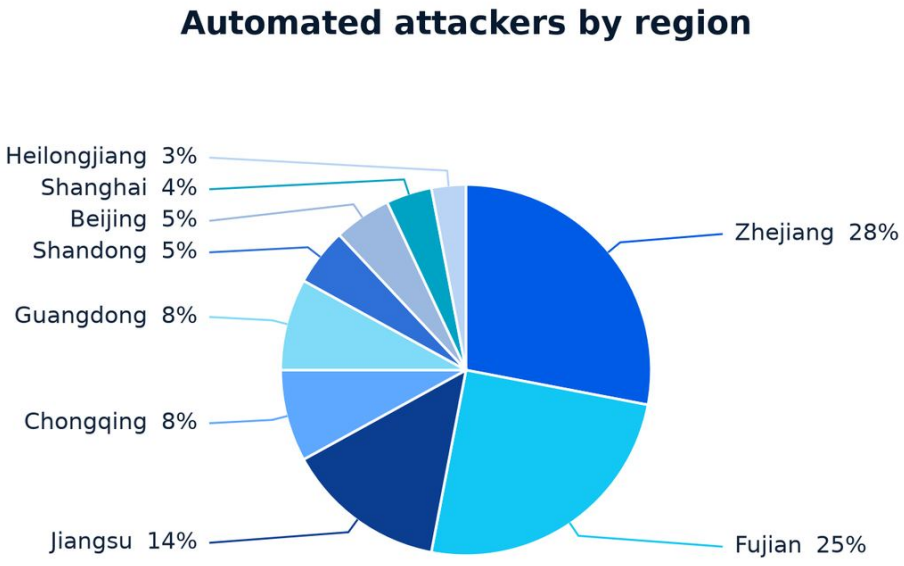
6. threat actors attack process automation systems

For threat actors, they will do everything they can to continuously reduce attack costs and improve attack efficiency. Automated attacks are one of the key methods.

In the current cybercrime ecosystem chain, from the upstream providing threat actor resources to the downstream using threat actor resources to launch attacks, a complete ecosystem with low coupling and high automation has been formed. Based on the network cybercrime ecosystem

intelligence recently captured by the Threat Hunter business intelligence monitoring platform, we analyzed the data, behaviors and technical principles of threat actors that meet the characteristics of automated attacks, and tried our best to show their full picture.

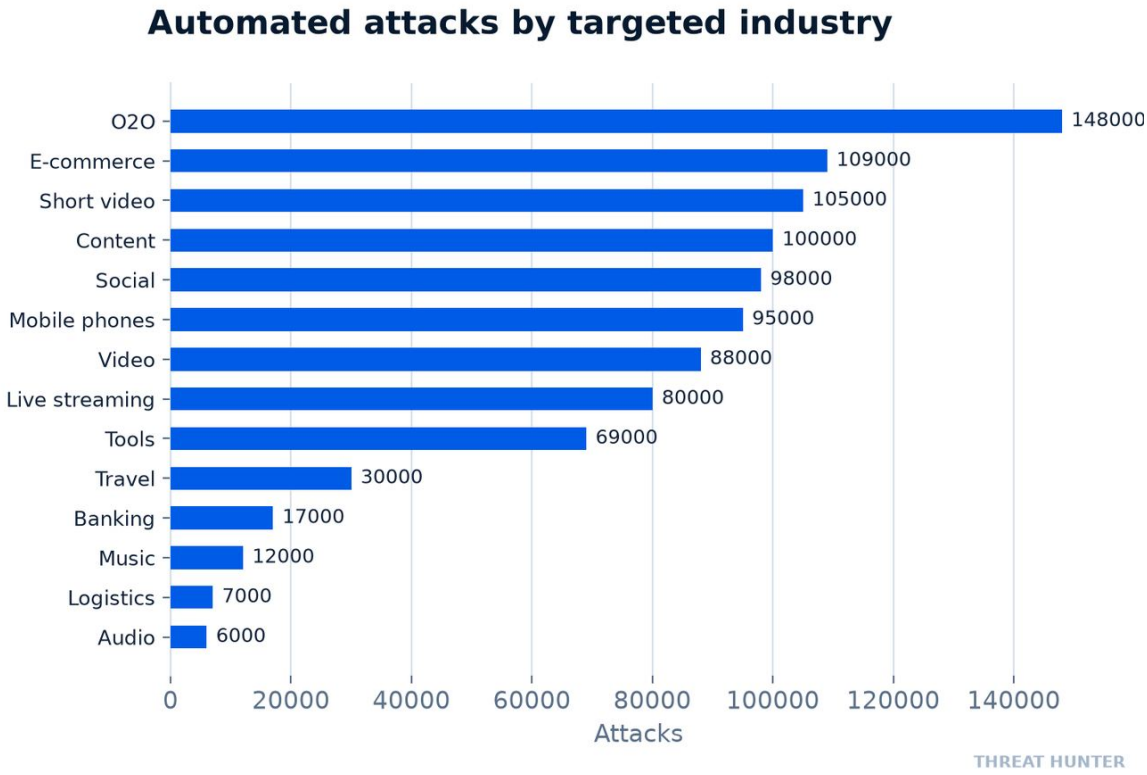
Judging from the geographical distribution of attackers, economically developed coastal areas, such as Zhejiang, Fujian, Jiangsu, Guangdong, etc., also have a higher proportion of automated attacks:



Automated attackers by region

Source: Threat Hunter original report, page 64. Redrawn in English from the original figure.

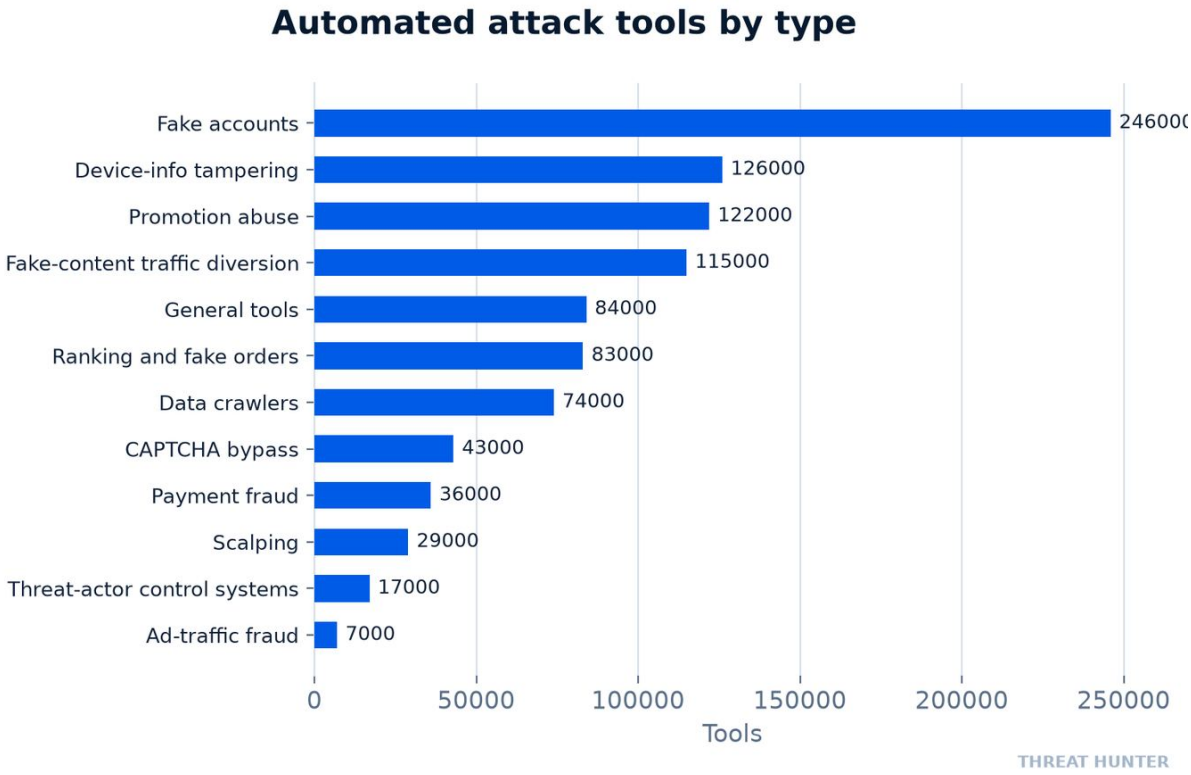
Judging from the distribution of industries attacked, O2O, e-commerce, short video and other industries where threat actors can benefit on a large scale are the hardest hit areas for automated attacks by threat actors:



Automated attacks by targeted industry

Source: Threat Hunter original report, page 64. Redrawn in English from the original figure.

From the perspective of attack behavior, batch registration, batch profiteering, volume traffic manipulation, order traffic manipulation, traffic diversion, etc. often require the control of a large number of accounts, so the dependence on automated attacks is stronger:



Automated attack tools by type

Source: Threat Hunter original report, page 65. Redrawn in English from the original figure.

6.1 Highly integrated automated attack process of threat-actor resources

In our previous reports, we have described in detail the various resources required by cybercrime ecosystem to launch attacks on companies' businesses, as well as the platforms that provide resources, including a SMS verification-code receiving service that provides mobile-number resources, a card issuance platform that provides account resources, an agent IP website and a dial-up platform that provide IP resources, and group control/cloud control/box control that provides device resources and device management. For ease of use, these resource platforms provide a variety of ways that threat actors can be seamlessly integrated and used downstream during automated attacks.

6.1.1 API interface

For the convenience of threat actors resource platform, the most typical way is to provide API interface, so that it can be called directly in automated scripts or programs. Taking the SMS verification-code receiving service as an example, there are two main API interfaces provided, one is to obtain a phone number and to obtain a verification code. The interface for obtaining phone numbers is generally defined as follows:

http://api. xxxxxx .com/api/do.php ? action=getPhone The parameter action=getPhone means to obtain the phone number. In addition, the parameter sid needs to be used to specify the project, that is, the product or business for which the phone number is to be registered. Some products have strict control over new user registration, and you can use the parameter exclude to exclude

the number segments of virtual operators; some activities are only targeted at certain areas, such as a new product promotion event held in Chengdu, and you can use the parameter location to specify the phone number in Chengdu.

The interface for obtaining verification codes is generally defined as follows:

http://api.xxxxxx.com/api/do.php?action=getMessage

The parameter action=getPhone means to obtain the verification code. In addition, the parameter sid also needs to be used to specify the project. The returned data format is generally: 1|SMS content, 1 indicates success. The SMS content contains the verification code. The verification code can be extracted through simple string matching or regular expressions, and then registration is performed.

[Tips] Since the API interfaces of each CAPTCHA-solving service have similar parameter formats except for the domain name, you can define some regular expressions to capture the API interface access traffic of the CAPTCHA-solving service from the traffic (such as our honeypot traffic), so that you can roughly grasp the number and scale of the CAPTCHA-solving services on the entire network.

Taking the proxy IP website as an example, they basically provide API interfaces. Compared with the API interface of the CAPTCHA-solving service, it is easier to use. As shown in the figure below, it is an API interface description provided by a proxy IP website:



API documentation of a proxy IP website

Source: Threat Hunter original report, page 66. Original image retained.

You only need to call an API interface, and the returned data is in json format, which can directly parse out the IP address and port.

In order to combat automated attacks, many companies often integrate verification codes into business processes to perform human-machine identification. Correspondingly, the cybercrime ecosystem also integrates automatic recognition of verification codes into automated attacks. Platforms that provide automatic identification of verification codes are generally called CAPTCHA-solving services or CAPTCHA-solving services. Whether it is a picture verification code, a sliding verification code or some complex verification codes, these platforms provide API interfaces for bypassing these verification codes. The picture below is one of the code-passing platforms, and the API usage instructions for bypassing a certain verification code:



API usage notes of a CAPTCHA service (1)

Source: Threat Hunter original report, page 67. Original image retained.

子程序名	返回值类型	公开	易包	备 注
极验识别	文本型			

参数名	类 型	参考	可空	数组	备 注
gt	文本型				所在网站极验的gt值
referer	文本型				所在的页面来源地址
challenge	文本型		✔		通过请求目标站配置项获取，每次获取到的challenge仅能使用一次。如网站为极验感知此参数可不填，比如拉钩

变量名	类 型	静态	数组	备 注
url	文本型			
secretkey	文本型			后台的接口访问密钥
body	文本型			
supporttype	文本型			
response	文本型			
http	WinHttpW			
ip	文本型			

```
url = "http://api.ddocr.com/api/gateway.jsonp"
' 这里替换为你的密钥，这个为必传
secretkey = "xxxxxxxxxxxxxxxx"
supporttype = "" ' 如果遇到特殊图像传supporttype =3 注意特殊图像比较贵 识别成功则扣30点
ip = "" ' 如果网站认ip，需要使用自己的ip的话传此参数，一般情况下不需要
body = "wtype=geetest&secretkey=" + secretkey + "&gt=" + gt + "&referer=" + referer + "&challenge=" + challenge + "&supporttype=" + supporttype + "&ip=" + ip
http.Auto (真)
' 设置60秒超时
http.SetTimeouts (3000, 3000, 3000, 60000)
http.Open ("POST", url)
http.Send (body)
response = http.GetResponseTextUtf8ToAnsi ()
调试输出 (response)
返回 (response)
```

永安在线反欺诈

API usage notes of a CAPTCHA service (2)

Source: Threat Hunter original report, page 67. Original image retained.

```
public class GeetestRecognition {

    private static final String api = "http://api.ddocr.com/api/gateway.jsonp";
    //这里为您的后台的首页的，开发者信息的接口秘钥
    private static final String secretkey = "";

    /**
     * @param gt 所在网站极验的gt值
     * @param referer 来源页面地址
     * @param challenge 通过请求目标站配置项获取，每次获取到的challenge仅能使用一次。如网站为极验感知此参数可不填，比如拉钩
     * @return
     */
    public static String recognition(String gt,String referer,String challenge){
        StringBuffer body = new StringBuffer();
        body.append("wtype=geetest&secretkey=").append(secretkey);
        body.append("&gt=").append(gt).append("&referer=").append(referer);
        body.append("&challenge=").append(challenge==null?"":challenge);
        //如果想使用自己的代理ip传进来即可
        body.append("&ip=");
        body.append("&proxyuser=");
        body.append("&proxypwd=");
        body.append("&supporttype=");//如果遇到特殊图片，请传3，其他则不用
        String resp = HttpUtils.getInstance().post(api, body.toString());
        return resp;
    }
```

永安在线反欺诈

API usage notes of a CAPTCHA service (3)

Source: Threat Hunter original report, page 67. Original image retained.



```php
<?php

require_once 'curl.func.php';

$appkey = 'your_appkey_here';//你的appkey
$pic = base64_encode(file_get_contents('11.jpg'));//验证码图片
$type = 'n4';//图片类型
$url = "https://api.jisuapi.com/captcha/recognize?appkey=$appkey";

$post = array(
    'pic'=>$pic,
    'type'=>$type
);
$result = curlOpen($url, array('post'=>$post));
$jsonarr = json_decode($result, true);

if($jsonarr['status'] != 0)
{
    echo $jsonarr['msg'];
    exit();
}

$result = $jsonarr['result'];
echo $result['type'].' '.$result['code'];
```

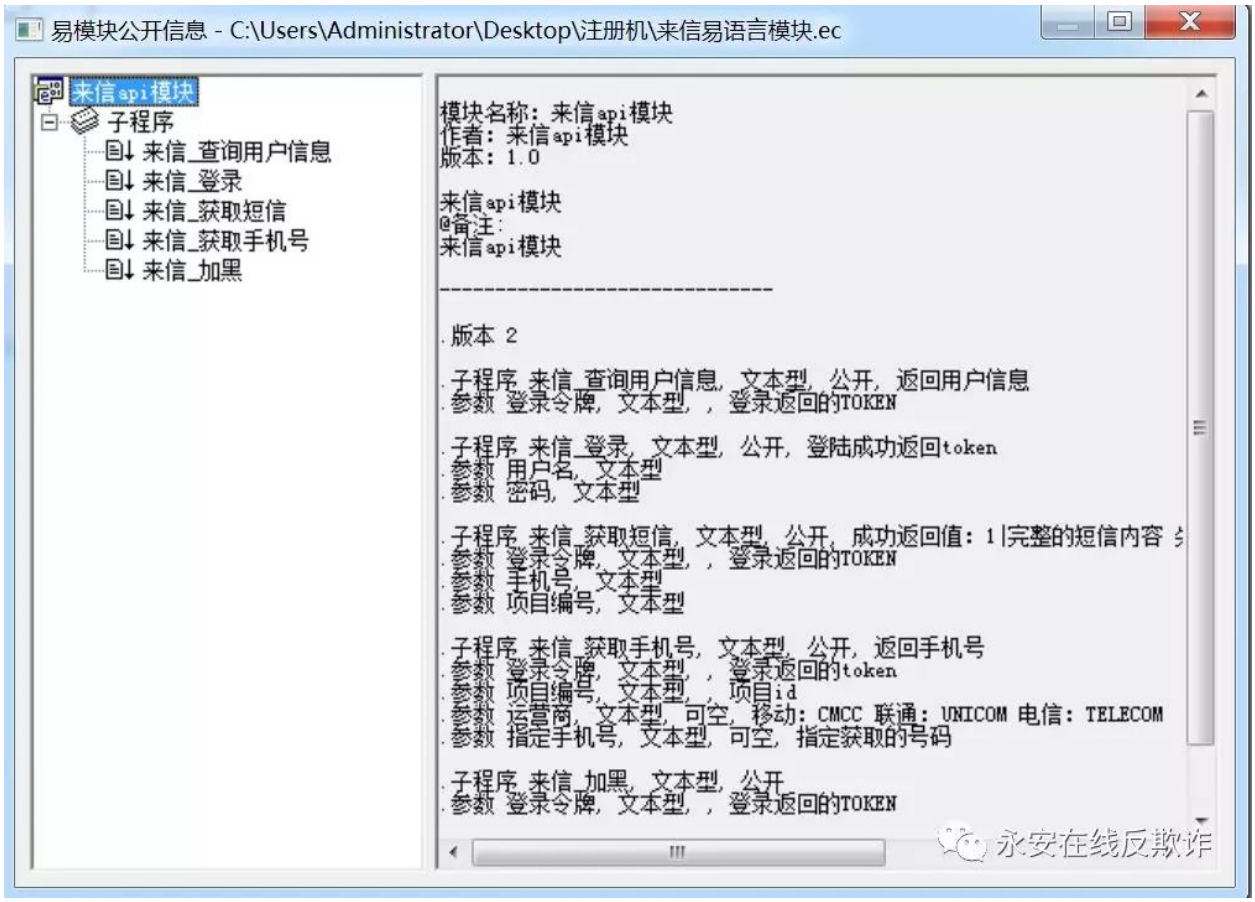
永安在线反欺诈

API usage notes of a CAPTCHA service (4)

Source: Threat Hunter original report, page 68. Original image retained.

6.1.2 Function module

For cybercrime ecosystem to implement automated attacks, the API interface is convenient enough, but the cybercrime ecosystem also pursues "excellence", so there is another more convenient way to directly provide encapsulated function modules. Since the vast majority of cybercrime ecosystem tool software is written in Easy Language, most of them provide modules encapsulated in Easy Language. Let’s still take the CAPTCHA-solving service as an example. The picture below shows the information exported by the easy language module (.ec) of a CAPTCHA-solving service. You can see that the required functions have been encapsulated:



An automated promotion-abuse tool written in Easy Language

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

Let’s take a recently discovered automated promotion abuse tool written in Yi language as an example. The code related to the code only requires a few lines of code:

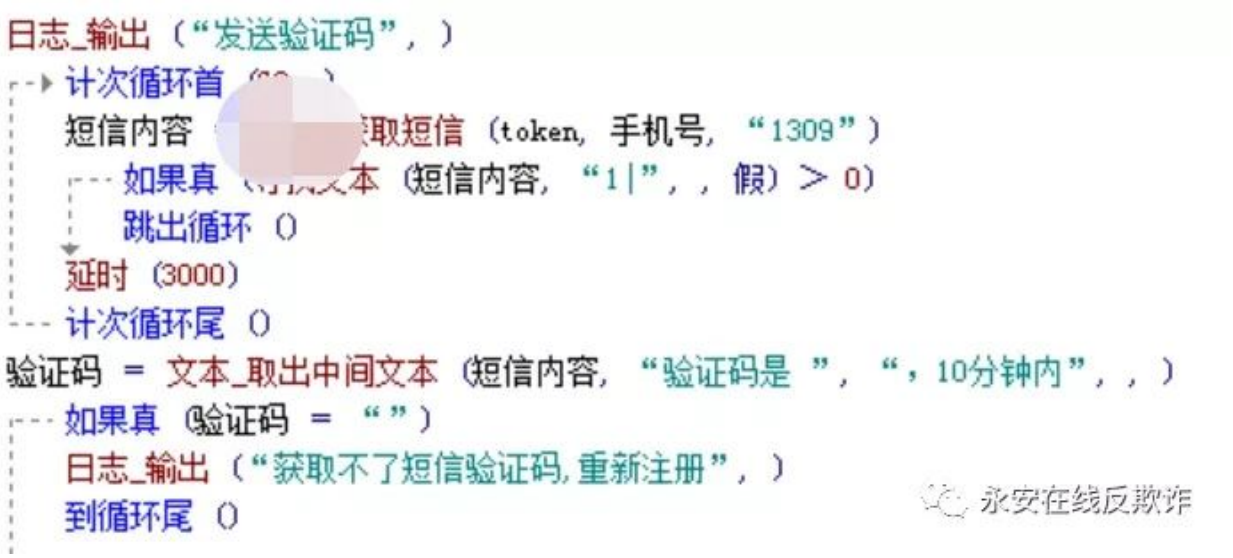
1) Log in to the SMS verification-code receiving service and obtain your phone number:



Easy Language code: log in to a code-receiving platform and get a phone number

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

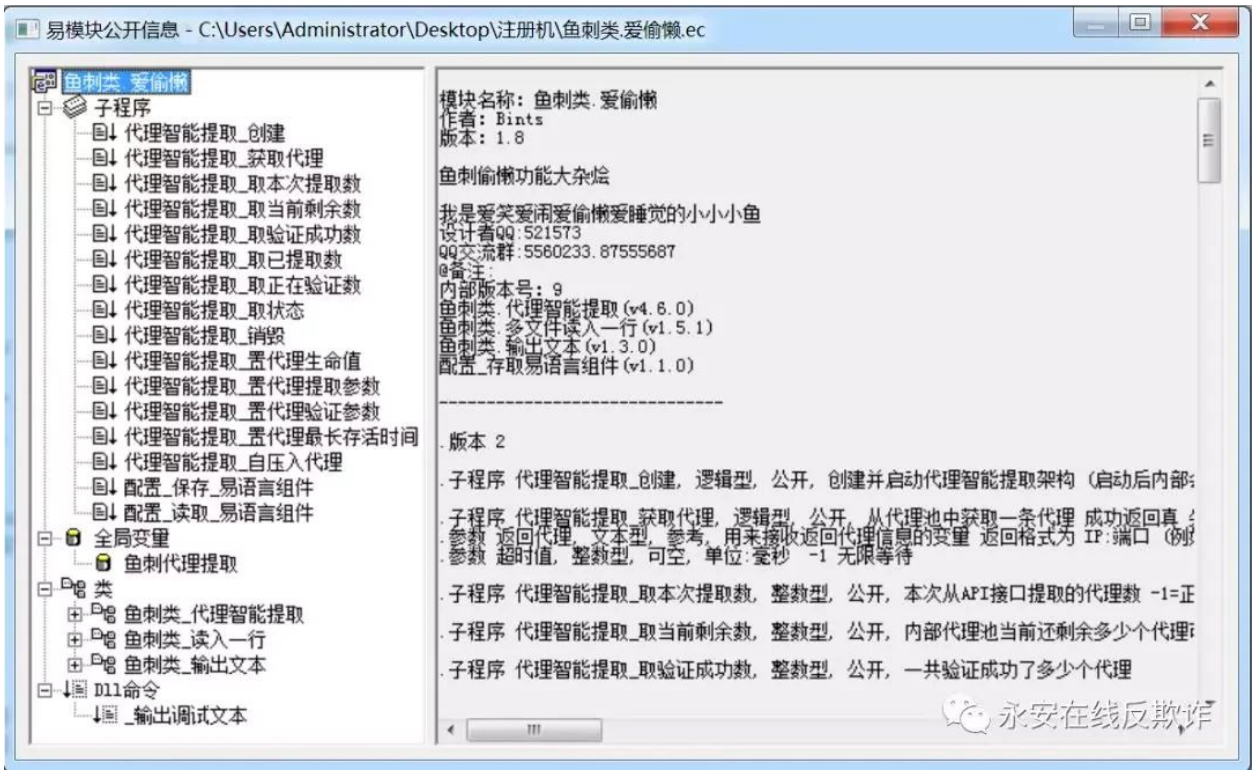
2) Get the verification code:



Easy Language code: get the verification code

Source: Threat Hunter original report, page 70. Original image retained.

For the use of proxy IP, there are also encapsulated functional modules that can be used, as shown in the figure below:

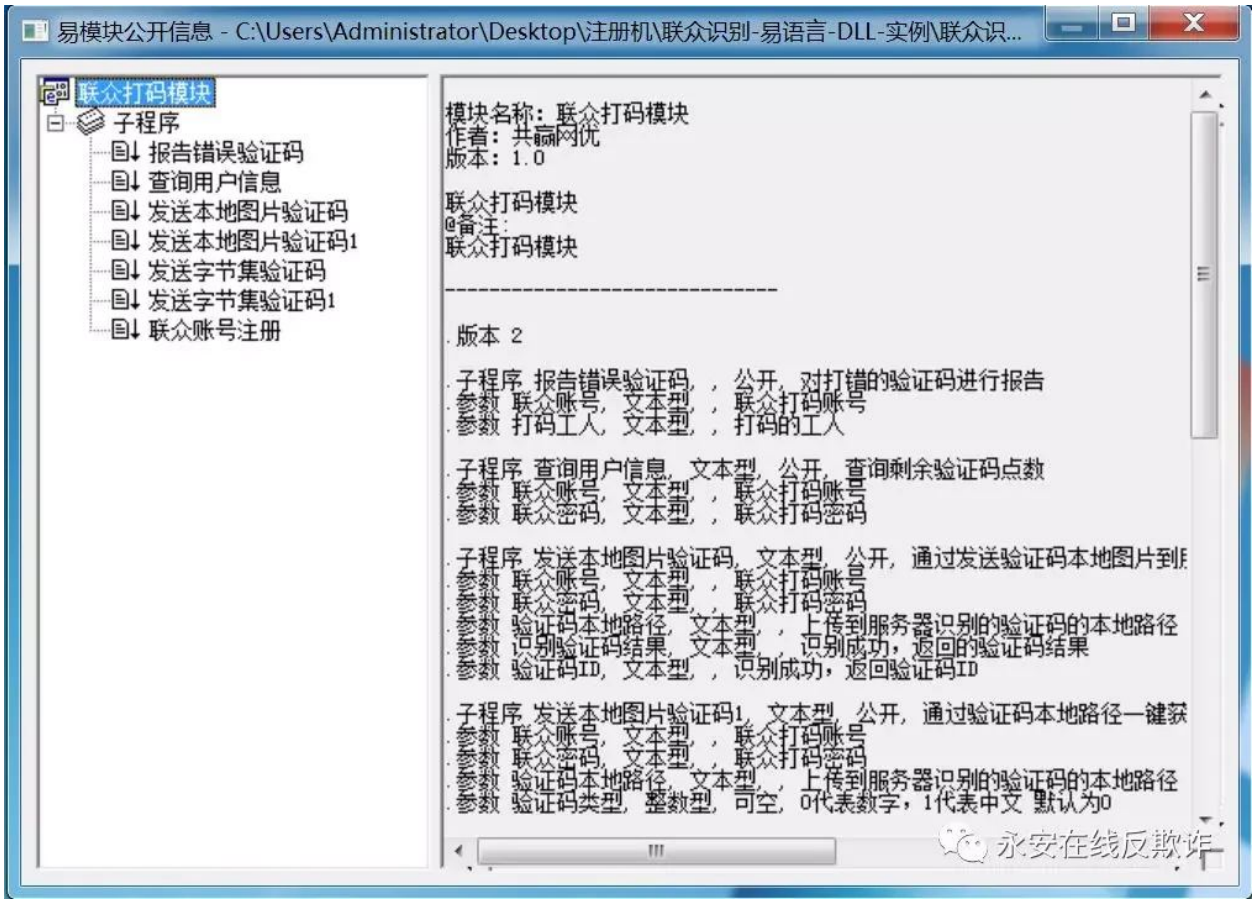


Ready-made proxy IP module for Easy Language

Source: Threat Hunter original report, page 70. Original image retained.

In addition to extracting the proxy IP, it also provides the function of verifying the validity of the proxy IP. Users no longer need to use other tools or write their own code to verify the validity of the proxy IP, which is "intimate".

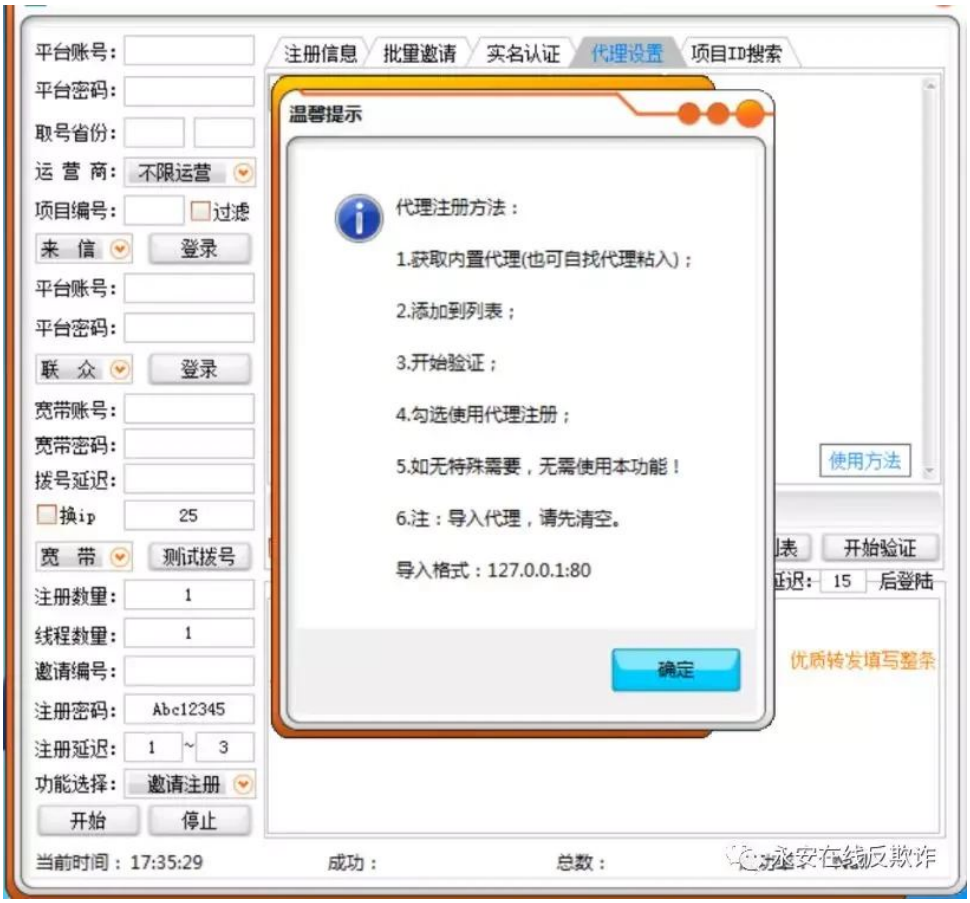
Some CAPTCHA-solving services also provide easy language function modules, as shown in the figure below:



CAPTCHA-solving module for Easy Language

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

The automated registration machine tool shown below, written in Yi language, can be said to be a typical "master", including the functional modules of the SMS verification-code receiving service, CAPTCHA-solving service, broadband dial-up, proxy IP and other threat-actor resources, all integrated into the tool. You only need to fill in the account and password of each threat actors resource platform on the interface and perform some simple configurations, and all automated attack processes can be carried out with one click.



An all-in-one automated registration bot

Source: Threat Hunter original report, page 72. Original image retained.

6.1.3 Provide environment

For platforms that provide IP resources, compared to proxy IP, Mdial is not only cheaper and has more available IP resources, it is also more convenient to use for automated attacks: there is no need to embed API interfaces or functional modules in scripts or programs, and automated attacks can be run directly in the environment provided by Mdial. There are two ways:

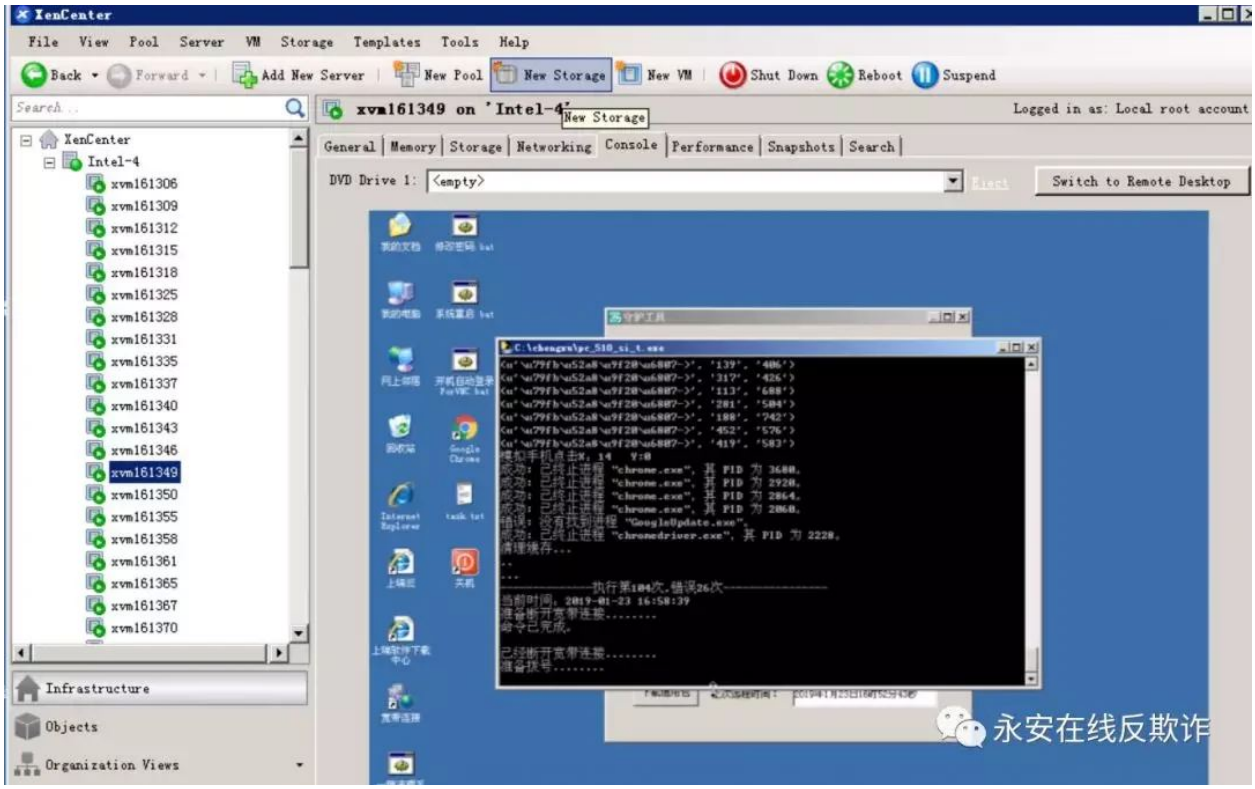
1) Start the instant dial client program, turn on automatic dialing, and then perform automated attacks:



Rapid dial-up client running alongside an automated attack

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

2) Run the automated attack script or program in Mdial VPS. Mdial VPS provides automatic dialing function:

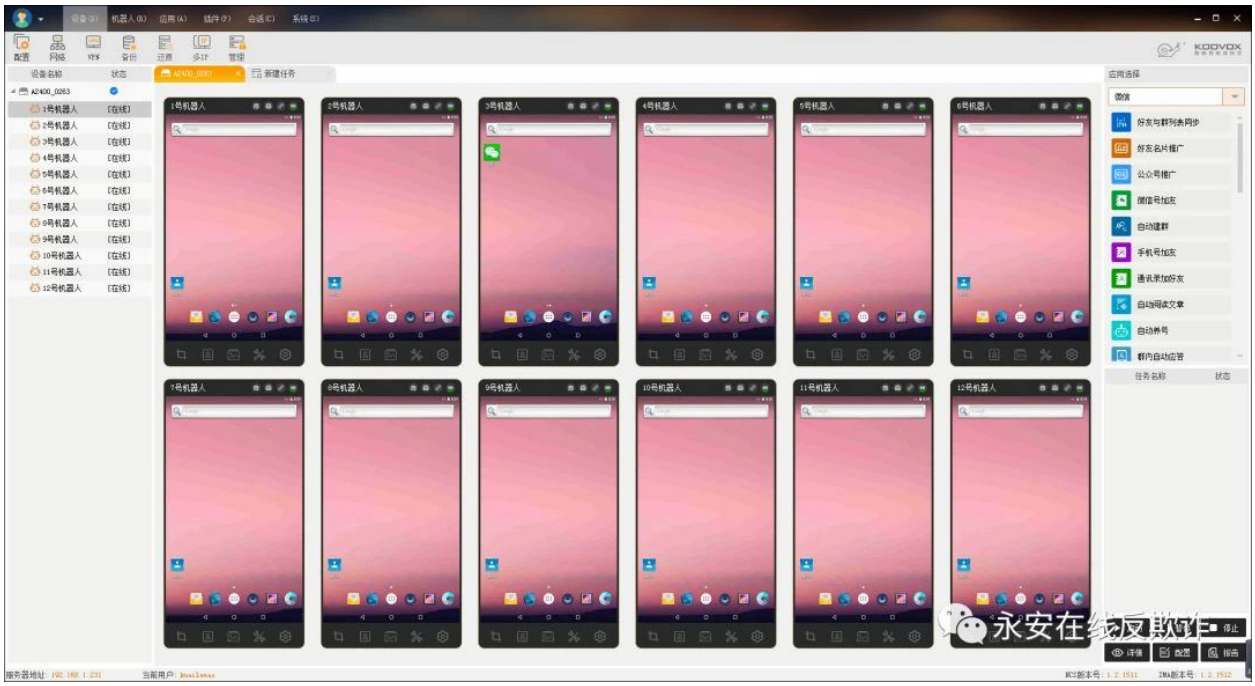


Automated attack script running on a rapid dial-up VPS

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

6.1.4 Integrated system

Providers of equipment resources for threat actors can be understood as hardware companies in the cybercrime ecosystem. In recent years, mobile phone hardware companies have not only continuously improved their hardware capabilities, but also continued to develop the software market. For example, the mobile phone system directly integrates its own application store, browser, mobile phone management software, etc., and users do not need to install additional devices. Similarly, for threat actors equipment providers, they no longer simply provide hardware equipment, but integrate various resources needed by cybercrime ecosystem to complete automated attacks. In terms of external packaging, slogans such as "one-stop marketing" and "private domain traffic marketing" are often used.



Box-control software with built-in attack functions

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

Let’s take a certain box-type group control as an example. As you can see directly from the picture below, this box control tool has built-in the following functions:

1)VPN dial-up function, you can easily switch IP;

2) The virtual positioning function can easily modify the positioning to realize false travel orders or solicit prostitution on the street;

3) The machine modification function can easily modify hardware parameters such as IMEI and IMSI, thereby forging more devices;

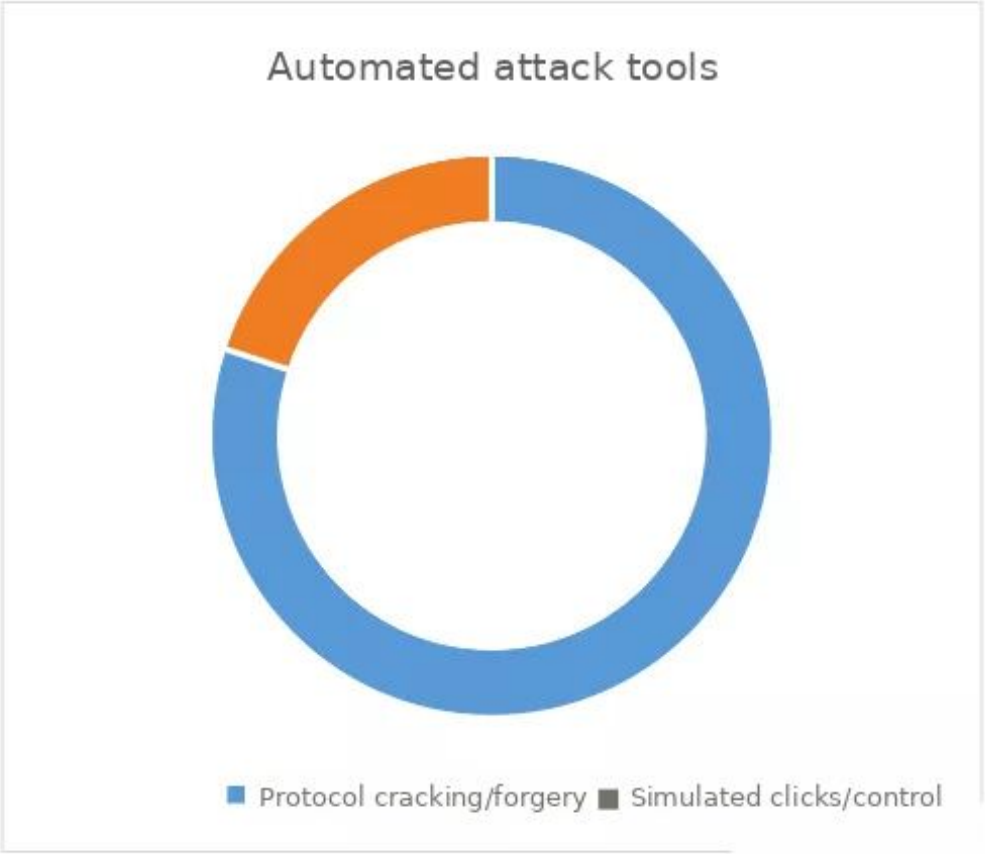
4) Mainstream mobile App automatic control scripts, such as a messaging app automatically adding friends, automatically adding groups, automatically posting to friend feeds, automatic following on short-video apps, automatic likes, automatic comments, etc.;

5) The cloud backup function can upload and back up the entire attack environment together with the account logged in to the environment, and switch environments by restoring snapshots to conduct a large number of attacks.

6.2 Technical means of automated attacks and offensive and defensive confrontations

threat actors implement automated attacks mainly through two technical means: protocol cracking/forgery, and simulated click/control.

The former requires cracking the interface protocol of the application first, which has a certain technical threshold and is relatively difficult; while the latter is simple to develop, highly readable, has a low threshold for getting started, and has a wider audience for threat actors. Among the automated attack tools we have captured recently, the proportion of simulated click/manipulation tools is also higher:



Automated attack tools: protocol cracking vs simulated clicks

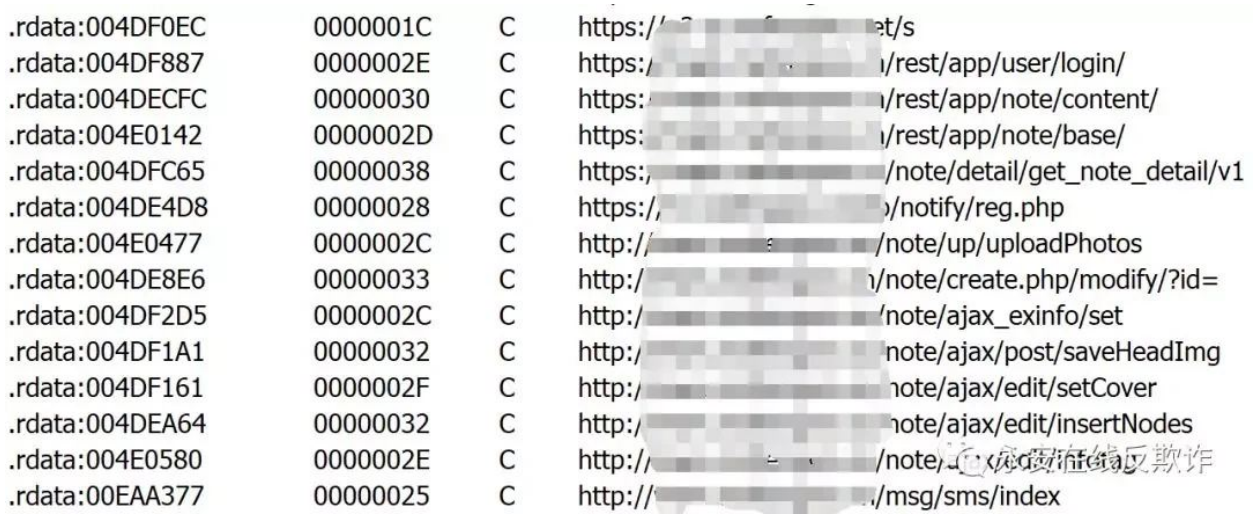
Source: Threat Hunter original report, page 75. Original figure with Chinese text replaced by English.

Next, we will introduce these two types of automated attack technologies in more detail.

6.2.1 Protocol cracking/forgery

Protocol cracking/forgery refers to obtaining the request interface and parameters for communication between the client and the server through packet capture + reverse analysis, etc., and directly forging the interface protocol and parameters to complete automated operations.

Let’s take an automatic posting machine for a travel application as an example. Through analysis, we can see that this posting opportunity automatically accesses many back-end interfaces of the application:



Back-end API paths found in a travel-app posting bot

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

Since the interface protocol and parameters have been cracked, all parameters have been constructed before accessing the interface:



Prebuilt request parameters in the posting bot

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

The cost of forging some of the parameters is not high, and they are even directly hard-coded in the code.

Some parameters will be dynamically generated according to certain rules to meet legality verification. Taking the two parameters os_api and os_version as an example, an os_version array is built into the code:

```
array_os_version_31B08F3 dd 1           ; DATA XREF: gen_os_
                         dd 9
                         dd offset a8_0_0       ; "8.0.0"
                         dd offset a5_1_0       ; "5.1.0"
                         dd offset a5_0_1       ; "5.0.1"
                         dd offset a5_1_1       ; "5.1.1"
                         dd offset a6_0_1       ; "6.0.1"
                         dd offset a5_0_0       ; "5.0.0"
                         dd offset a4_4_4       ; "4.4.4"
                         dd offset a810_0       ; "8.1.0"
                         dd offset a4_4_1       ; "4.4.1"
```

永安在线反欺诈

Built-in os_version array

Source: Threat Hunter original report, page 77. Original image retained.

When constructing parameters, the value of os_version will be randomly selected based on this array, and the value of os_api will be adapted based on the value of os_version:

```
v22 = sub_405FCE(v37, "6.0") == 0;
if ( v37 )
  j__krnl_MFree(v37);
if ( v22 )
  return "23";
v8 = *a2;
if ( !*a2 )
  v8 = &unk_64E2AC;
v38 = (_BYTE *)j__krnl_MCallKrnlLibCmd(2, (char)v8);
v23 = sub_405FCE(v38, "5.1") == 0;
if ( v38 )
  j__krnl_MFree(v38);
if ( v23 )
  return "22";
```

永安在线反欺诈

Matching os_api to the chosen os_version

Source: Threat Hunter original report, page 77. Original image retained.

Another example is the two parameters device_type and device_brand. A large array of device types is built into the code:



Built-in array of device types and brands

Source: Threat Hunter original report, page 78. Original image retained.

When constructing parameters, random selection is also performed. If the first element of the array is selected, the generated parameters are device_type=B7330 and the matching device_brand value.

The parameters listed above are relatively simple to forge, but there are some parameters that are much more difficult to forge. Especially for some applications that have protocol protection, there will be parameters specifically used to verify the legitimacy of interface requests, and multiple parameters will be verified against each other. As long as one of the parameters is constructed incorrectly, it will not pass the verification.

In theory, threat actors seem to be deterred by the increased cost of confrontation, but in reality this is not the case.

First of all, on open source or free channels, code-hosting sites and developer forums have a large number of explanations of the principles of protocol algorithms and even code cracking. Although the author's starting point may be purely technical discussion, it is directly exploited by threat actors with ulterior motives:



Signing-algorithm cracking code shared on a code-hosting site

Source: Threat Hunter original report, page 79. Original image retained.

Secondly, there are some cracking websites that have specialized technical personnel behind them and also provide paid algorithm cracking services:



Paid algorithm-cracking service

Source: Threat Hunter original report, page 79. Original image retained.

In addition, although with the development of mobile application reinforcement technology (including mature commercial products and solutions), it is becoming more and more difficult to crack the core algorithm. However, due to the asymmetry between offense and defense, threat actors can bypass this line of defense and choose to attack the weak points of the defense. Web-side applications have become such a breakthrough. Although the code of the Web front-end can be obfuscated and encrypted, it is relatively difficult to crack. You can even directly extract the key code of the algorithm without cracking it, and call and execute it through the script engine to complete the construction of encryption parameters:

```
var CryptoJS = CryptoJS || function (u, p) {
    var d = {}, l = d.lib = {}, s = function () {
        }, t = l.Base = {extend: function (a) {
            s.prototype = this;
            var c = new s;
            a && c.mixIn(a);
            c.hasOwnProperty(\"init\") || (c.init = function () {
                c.$super.init.apply(this, arguments)
            });
            c.init.prototype = c;
            c.$super = this;
            return c
        }, create: function () {
            var a = this.extend();
            a.init.apply(a, arguments);
            return a
        }, init: function () {
        }, mixIn: function (a) {
            for (var c in a)a.hasOwnProperty(c) && (this[c] = a[c]);
            a.hasOwnProperty(\"toString\") && (this.toString = a.toString)
        }, clone: function () {
            return this.init.prototype.extend(this)
        }},
```

永安在线反欺诈

Calling the app's own encryption code through a JavaScript engine

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

For companies, since protocol cracking/forgery is beyond the constraints of the environment and equipment, cybercriminal groups can complete batch and large-scale crimes at a very low cost, so the harm is more serious. How to prevent or detect such automated attacks more effectively, in addition to strengthening the complexity of the core algorithm, you can also try to start with intelligence. As mentioned earlier, in the fake interface protocol, some parameters are hard-coded. Based on these hard-coded parameters, feature clustering and analysis can be done, and identification rules can be extracted in a targeted manner. In addition, when threat actors construct the code for automated attacks, they are not seamless and often leave loopholes in some places. One of the more typical situations is that when accessing different interfaces, the constructed parameters are inconsistent. For example, the device type passed in the login request is an iOS device:

```
'http://[redacted]'2/auth/login/v2/?platform=[redacted]'
                ; DATA XREF: sub_4AAF55+111↑o
'[redacted]&iid=&device_id=&ac=&channel=yingyonghui&aid=1128&ap'
'p_name=aweme&version_code=144&version_name=1.6.8&device_'
'platform=iPhone&device_type=&device_brand=&os_api=22&os_'
'version=5.1.1&vid=&openudid=&manifest_versio[redacted]'
'&resolution=720*1280&dpi=192&update_version_code=16807',0
```

永安在线反欺诈

Login request claiming an iOS device

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

But then when registering the device, the registration information changed to say that the operating system is Android and the device maker is a different phone vendor:



Device registration claiming Android on another vendor's phone

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

Through this intelligence information, the identification of automated protocol cracking/forgery attacks can be continuously supplemented and improved.

6.2.2 Simulate click/control

Simulating click/control refers to completing operations such as input, click, and movement of interface controls by triggering mouse/keyboard/touch events, or through code injection, etc. If the confrontation of protocol cracking/forgery is a head-to-head confrontation of technology, simulated click/control can be said to be a victory through cleverness, and due to the low threshold for getting started, it has become the most popular automated attack method of the current cybercrime ecosystem. Next, we will explain several common simulated click/control attack methods.

1) Key Genie Key Genie is a well-known old automation script tool that everyone is very familiar with. It is also the most commonly used tool by threat actors to implement automated attacks by simulating clicks. By writing relevant logic scripts, cybercrime operators can simulate user operations to achieve the functions they want, such as mobile phone touch and button operations; they can also manually "record" the functions they want to operate first, so that the button wizard will automatically record the operation behavior sequence and coordinate trajectory, which is very convenient.

Let's take a traffic diversion tool of a certain short video platform as an example. This tool is an apk file generated based on the Button Wizard (Android version) script package. Its main function is to automatically like and comment on short videos on the platform, and send private messages to users, thereby achieving the traffic diversion effect, as shown below:



A short-video traffic-diversion tool

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

When using this tool, as long as you open the fan list interface of an Internet celebrity's homepage on the short video platform, you can automatically open each fan's homepage in order, like the video, comment on the video, and send private messages to the fan. Moreover, the tool also supports custom configurations, such as whether to follow fans, custom traffic-drawing words, etc.

2) Auto.js If Button Wizard is the old elite, Auto.js can be said to be a rising star. According to intelligence, starting around the end of 2018, more and more cybercrime operators are using Auto.js to develop automated attack scripts. Auto.js is a JavaScript-based automation script framework for the Android platform. Compared with the key wizard, Auto.js has the following advantages:

1) The device does not require Root, the cost of use is lower, and it can avoid Root-based risk device environment detection;

2) Button Wizard implements simulation operations based on identifying pictures, colors, coordinates, etc., and has resolution compatibility issues, while Auto.js can directly operate controls, automatically adapt to various Android models, and has higher stability;

3) The apk file generated by using Auto.js development and packaging is smaller in size.

Let's take an automated script for adding group members and friends on a social platform as an example. First, determine whether you are in a group chat window:

```
launchApp(    );
sleep(500);
if(currentActivity() != "com.    .activity.TroopMemberListActivity"){
    toast("请打开要加的群的聊天窗口");
    openGroupMemberList();
}
```

永安在线反欺诈

Script check for the group-chat window

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

After obtaining the messaging-app ID of the group member, click "Add Friend", fill in the verification information, and send the request automatically:

```
function addAsFriend(){
    var qq = getQQ();
    toast(qq);
    if(added[qq]){
        while(!click("返回"));
        return;
    }
    added[qq] = true;
    if(click("加好友")){
        sleep(800);
        setText(0, 好友验证信息);
        while(!click("发送"));
        sleep(800);
        if(click("取消")){
          sleep(400);
        }
        while(!back());
    }else{
        while(!back());
    }
}
```

永安在线反欺诈

Script that adds group members as friends

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

Auto.js script developers can use a code editor with the Auto.js plug-in to develop scripts. When the computer is connected to a mobile terminal, they can directly control the mobile phone with the Auto.js client to execute the script. They can also save the script to the mobile terminal, compile it into an APK, and run the APK to execute the operation.

3) Browser kernel For web-side applications, the cybercrime ecosystem often uses the browser as the carrier of automated attacks. One way is to embed the browser kernel in the tool. Take Chromium as an example. In order to provide embeddable browser support for third-party applications, an open-source project was created: CEF, which stands for Chromium Embedded Framework.

CEF isolates the complex code of the underlying Chromium and Blink, and provides a set of product-level stable APIs, releases branches that track specific Chromium versions, and binary packages. Most features of CEF provide rich default implementations, allowing users to meet their needs with as little customization as possible. One of the application scenarios of CEF is for automated web testing, which also opens the door to cybercrime ecosystem for automated attacks.

Let's take a smart crawler collector as an example. The software has a built-in Chromium browser and can complete automated operations by directly manipulating page controls. The crawler collector is very simple to use. You only need to enter the target website in the software interface, and you can crawl the data of the target website according to your needs. The interface is as follows:



Interface of a smart crawler collector

Source: Threat Hunter original report, page 84. Original image retained.

Use this tool to crawl data from a travel website as follows:



导出状态	序号	标题	标题链接	缩略图	detail1	detail2	location	view
	1	第一次去泰国，一...	http://www.	http://b1-q	Q 如何办理泰国签...	Q 去泰国需要买旅...	泰国	446669
	2	干货！普吉岛岛民...	http://www.	http://n1-q	NO.1选西不选东，...	西海岸南部最方便	普吉岛	60533
	3	值得收藏！保姆式...	http://www.	http://p1-q	一、护照	二、签证	泰国	184376
	4	落地签免签证费～...	http://www.	http://n1-q	支付宝可办理泰国...	落地签证是什么？	泰国	369
	5	超详细易懂的泰国...	http://www.	http://b1-q	图片目录（看图片...	前期准备	泰国	37172
	6	泰国猛男餐厅升级p...	http://www.	http://n1-q	猛男酒店：华富里P...	监狱酒店：曼谷So...	泰国	145
	7	曼谷必游经典、网...	http://www.	http://n1-c	★经典必去景点	大皇宫	曼谷	129683
	8	第一次去泰国怎么...	http://www.	http://b1-q	第一次出境游为何...	泰国旅游地那么多...	泰国	710732
	9	曼谷+甲米6天自由...	http://www.	http://p1-q	行程规划：上海✈...	1、先说说航空公司	泰国	92390
	10	三天时间，教你怎...	http://www.	http://b1-c	初识清迈	1.清迈在哪里	清迈	245015
	11	手把手教你填写泰...	http://www.	http://p1-c	一、办理落地签需...	二、快速办理落地...	泰国	20974
	12	泰国购物|泰国这些...	http://www.	http://n1-q	外用篇	草药足贴	泰国	242192
	13	吐血整理！实测23...	http://www.	http://b1-q	01、小老板海苔	02、泰好吃榴莲干	泰国	65864
	14	泰国落地签免签证...	http://www.	http://b1-q	准备资料	填写说明	泰国	6329
	15	泰国王权免税店全...	http://www.	http://n1-q	在王权免税店购物...	买什么划算？	泰国	355251
	16	泰国旅游实用帖 | 物...	http://www.	http://p1-q	蜈蚣丸	老虎贴	泰国	72984
	17	7天时间，告诉你怎...	http://www.	http://p1-q	初识"曼清"	为什么7天时间最合...	曼谷	52390
	18	烧脑的泰国落地签...	http://www.	http://n1-q	所需的材料	机场办理	泰国	57026
	19	泰国购物买什么？3...	http://www.	http://p1-q	一、必买泰国本地...	1、Soffell驱蚊液	泰国	22613
	20	如何兑换泰铢	http://www.	http://n1-q	国内兑换	当地兑换	泰国	642201

永安在线反欺诈

Data crawled from a travel website

Source: Threat Hunter original report, page 84. Original image retained.

4) Automated Web Testing In order to facilitate automated Web testing, mainstream browsers themselves have also shown sufficient openness. For example, the familiar automated testing tool Selenium/WebDriver is based on some open features of the browser to complete automated control of Web pages. It is also very common for cybercrime ecosystem to use Selenium/WebDriver to complete automated attacks. For companies, they often embed a JavaScript script in the web code to detect this type of automated testing tools:

```
"value": function ()
{
    var a = common_func.map(
    [
        common_func.some(["phantom", "_phantom", "callPhantom", "webdriver", "_Selenium_IDE_Recorder", "_selenium",
        {
            return r in window
        }),
        common_func.some(["__driver_evaluate", "__webdriver_evaluate", "__selenium_evaluate", "__fxdriver_evaluate"
        {
            return r in document
        }),
        common_func.some(["selenium", "webdriver", "driver"], function (r)
        {
            return document.documentElement.getAttribute(r)
        }),
        new RegExp("PhantomJS", "i").test(navigator.userAgent),
        !!navigator.webdriver
    ],
```

永安在线反欺诈

Automated web-testing code abused by threat actors

Source: Threat Hunter original report, page 85. Original image retained.

In addition to the above, there is another means of automated web testing: browser remote debugging, which is also used by cybercrime ecosystem for automated attacks. Let's take the

account registration machine of a certain community software as an example. This tool will open the browser through remote debugging:

```
asc_4EB4A3      db '浏览器已创建，当前配置全部无效',0  ; DATA XREF: sub_419222+2B↑o
aCProgramFilesX_0 db '兄弟，(C:\Program Files (x86)\Google\Chrome\Application\chrome.exe)默'
                                        ; DATA XREF: sub_419222+90↑o
                db '认路径没浏览器呀',0
aRemoteDebuggin db '--remote-debugging-port=#引号',0
                                        ; DATA XREF: sub_419222+E2↑o
asc_4EB538      db ' ',0                ; DATA XREF: sub_419222+171↑o
                                        ; sub_419222+27C↑o ...
aUserDataDir    db '--user-data-dir=#引号',0
                                        ; DATA XREF: sub_419222+1ED↑o
aIncognito      db '--incognito',0      ; DATA XREF: sub_419222+2B6↑o
aStartMaximized db '--start-maximized',0
                                        ; DATA XREF: sub_419222+35C↑o
aProxyServer    db '--proxy-server=#引号',0
                                        ; DATA XREF: sub_419222+41B↑o
aUserAgent_1    db '--user-agent=#引号',0 ; DATA XREF: sub_419222+4ED↑o
aNoFirstRun     db '--no-first-run',0   ; DATA XREF: sub_419222:loc_4197BE↑o
asc_4EB5A5      db ',',0                ; DATA XREF: sub_419222+6B2↑o
                                        ; sub_419222+805↑o ...
aWindowPosition db '--window-position=#引号',0
                                        ; DATA XREF: sub_419222+6BA↑o
aWindowSize     db '--window-size=#引号',0
                                        ; DATA XREF: sub_419222+80D↑o
```

永安在线反欺诈

Registration bot opening a browser through remote debugging

Source: Threat Hunter original report, page 85. Original image retained.

The browser is then controlled through WebSocket communication. Includes:

- Execute document.querySelector('[name=username]').select() to get the focus of the phone number input box;
- Send the Input.dispatchKeyEvent message and automatically fill in the phone number obtained from the SMS verification-code receiving service;
- Execute document.querySelector(‘button.Button.CountingDownButton.SignFlow-smsInputButton.Button--plain’).click() and click the “Get SMS Verification Code” button;
- Execute document.querySelector('[name=digits]').select() to get the focus of the verification code input box, automatically fill in the verification code, and execute document.querySelector('button.Button.SignFlow-submitButton.Button--primary.Button--blue').click() to click the "Register/Login" button.

Simulated click/control attacks on the mobile side require the attacked mobile application to be run on the device.

Moreover, if you want to implement batch and large-scale attacks, you need a large amount of equipment resources (group control, cloud control, box control, or forging equipment resources through simulators/modification tools). Therefore, companies can conduct risk detection from the equipment environment level. Whether you use tools such as button sprites, Auto.js, machine modification tools, GPS forgery, or device environments such as simulators and group control, you can find clues from the device fingerprint data. In addition to being used as unique identifiers, device fingerprints should also have the ability to identify risk scenarios such as basic application multi-opening, machine modification environment/environment forgery, Hook behavior, Root/jailbreak, proxy/VPN and other risk scenarios. If you have strong intelligence capabilities, you

can collect as many automated attack script programs as possible, and detect whether such programs exist in the installation list (Applist) when the application starts.

On the other hand, although simulated click/manipulation attacks will imitate normal users' operating behaviors, they will still be different from the users' actual behavioral characteristics, and can be detected from the behavioral level.

For example, if you use a tool to boost store visits on an e-commerce platform, each boosting behavior will definitely include "open the homepage", "search for product keywords in the target store", "first enter two stores with similar products to browse the products" (imitating the habit of normal users to compare shopping), "complete the boost after entering the target store and browsing the products", and the time spent on each page is also fixed.

Extracting key user behavior features from business data for cluster analysis can effectively identify programmed simulation operations.

Another example is the above-mentioned smart crawler collector. Although it produces seemingly normal page browsing behavior, there are no normal mouse clicks, keyboard inputs or screen touches, which is also highly suspicious behavior.

Of course, device-level and behavioral-level data are often complementary. In order to ensure high accuracy and recognition rate, the determination of risk behaviors must be based on comprehensive judgments from multiple dimensions.

6.3 Attack and defense suggestions

Technically achieving a high degree of automation in the attack process is the inevitable way for cybercrime ecosystem to improve operational efficiency and reduce operating costs.

Stable and mature automated testing tools and technologies are abused by threat actors, which greatly improves the development and attack efficiency of threat actors. This will undoubtedly continue to face greater challenges for companies' business security protection strategies. Fortunately, the confrontation of human-machine recognition is a process of continuous upgrading and evolution. Whether it is for the business side or for the cybercrime ecosystem, there is no absolute silver bullet.

In addition to working on the fraud-control rule model, the business side can also perform risk detection on the equipment:

1) Detect the equipment environment in which the business is running. cybercrime ecosystem requires the use of some special operating environments whether it is spoofing device information or running automated script tools. Through analysis of these environments, some common detection points can generally be found.

For example, machine modification tools can detect Hook frameworks, and simulated clicks can detect system parameters. These can be used as suspicious device characteristics for weighted scoring.

2) Identify user behavior in business. The protocol simulation technology and simulated button technology commonly used in threat actors' automation are hugely different from the operating paths of natural humans. For example, when a user logs in, the input of the account and password will not be completed instantly, or the button will not be clicked in the same position every time. These can all be used as detection features. When we identify user operation behaviors, this greatly increases the cost of cybercrime ecosystem confrontation.

In the future human-machine confrontation, enterprises will face more and more automated attacks.

In terms of in-depth defense of business security, in addition to the construction of basic fraud controls, enterprises also need to carry out protection on the equipment, so as to increase the attack cost of threat actors and improve the protection effect.

4. Intelligence analysis of threat-actor tools

For enterprises, threat actors tool intelligence can effectively improve the offensive and defensive efficiency of business security. Through the business interfaces utilized by the analysis tools, not only can the malicious behavior of threat actors be effectively tracked and dealt with effectively, but also the business level's understanding of security can be strengthened, the security weaknesses in the business interfaces can be known, and continuous security reinforcement can be carried out.

1. Rapid analysis and validity verification of tool samples

Due to environment dependencies, component dependencies, resource dependencies, etc., the proportion of tool samples that can be manually run and perform corresponding functions is not high. The vast majority of tool samples can be quickly analyzed and validated through other methods, and the remaining small number of unknown samples or high-value samples can be reproduced through manual operation.

The main reasons why it is not easy to execute and reproduce the function manually are as follows:

1) Lack of environment for tool running, for example, tools written in .net require .net runtime environment, XPosed programs require XPosed framework, etc.;

2) Lack of some components that the tool depends on for running, mainly appearing in some PC-side tool samples, requiring some other dynamic library (DLL) support during runtime;

3) The tool will detect the virtual machine environment when running, resulting in the inability to run in the virtual machine, which mainly occurs in some PC-side tool samples;

Note: There are virus camouflage tools and virus-containing packaging tools in the tool samples. Therefore, when running the tool, be sure to place it in a virtual machine environment to prevent infection of the physical machine environment;

4) The tool requires activation or registration before it can be used. In this case, you can try to contact the author to purchase, or bypass activation or registration through cracking and other means and directly enter the main interface of the tool;

5) When the tool performs corresponding functions, it lacks the required resource files. For example, some tools need to read local account resource files when performing operations such as batch replying, likes, and following;

6) When the tool performs the corresponding function, it needs to purchase the resources of the threat-actor platform, such as registration machine tools. It is often necessary to register an account on the SMS verification-code receiving service and recharge it, and then fill in the account password of the SMS verification-code receiving service when the tool is running;

7) The traffic executed by the tools is relatively complex. Some need to be executed step by step according to certain steps, and some need to perform some pre-operations first. For this type of tool, you often have to find a tutorial first and follow the tutorial.

1.1 Analysis of PC-side tools

1.2.1 Search for "http:" and "https:"

Most of the PC-side tool samples are protocol tools (directly forging the communication protocol between the front-end and the server to complete batch automation operations). We can search for strings starting with "http:" and "https:" in the tool's built-in strings. If the searched string contains the interface URL of the corresponding business, as shown below:



Searching a PC tool’s strings for http and https

Source: Threat Hunter original report, page 89. Original image retained.

It can basically be concluded that the tool is a protocol tool.

1.2.2 Hard-coded parameters

After clarifying the protocol tools, the next step is to verify the effectiveness of the tools. Most protocol tools will have some hard-coded request parameters. These hard-coded parameters can often be found in the tool's built-in strings near the interface URL, as shown below:



Hard-coded parameters near an API URL

Source: Threat Hunter original report, page 89. Original image retained.

Use these hard-coded parameters as filter conditions to filter the interface traffic. If there is hit traffic, it means that the tool (or similar tools) has made a protocol request for the interface URL. At the same time, you can further observe whether these requests can be identified as malicious requests. If they are not identified, it means that the current tool is effective.

1.2 Analysis of mobile tools

1.2.1 Tool package name

Mobile tools mainly focus on simulated control, so before running the tool, you need to install the target App and run it. If the target App collects the App List containing package name information on the terminal device, it can be retrieved through the package name of the tool.

Recognize it. Drag the downloaded tool into an analysis tool such as a decompiler to obtain the package name information (we will also display the package name of the tool on the intelligence platform in the future):



Finding a tool's package name

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

If this tool is available on the terminal device, the device can be considered a high-risk device and necessary restrictions will be imposed on the service requests initiated by it.

1.2.2 Tool source code

Most mobile tools can download the source code restored through certain technical means on the intelligence platform. Reading the source code directly can clearly understand the operating principle of the tool, the resources it depends on, and the execution steps. Illustrated with 3 different types of tools:

1) The source code restored by the key wizard is a Lua script, and the amount of code is relatively large, often hundreds of K. When analyzing, you can start reading from the main function (usually at the end of the source code) to quickly understand its core functional logic. The following is the main function code snippet of a short video application red envelope tool:

```
;(function()
  local L0_1965
  L0_1965 = nil
  id494e5458, id494e5459, L0_1965 = LuaAuxLib.FindPicture(0, 0, 0, 0, "Attachment:滑块.png", "000000", 0, 0.9)
  return L0_1965
end)()
if id494e5458 > -1 then
  LuaAuxLib.TracePrint("_28:", "找到验证码")
  ide6bb91e58aa8()
  LuaAuxLib.Sleep(10000)
  LuaAuxLib.Swipe(519, 1565, 519, 465, 1000)
  LuaAuxLib.Sleep(3000)
  ;(function()
    local L0_1966
    L0_1966 = nil
    id494e5458, id494e5459, L0_1966 = LuaAuxLib.FindPicture(0, 0, 0, 0, "Attachment:滑块.png", "000000", 0, 0.9)
    return L0_1966
  end)()
  if id494e5458 > -1 then
    break
  end
else
  LuaAuxLib.TracePrint("_38:", "没找到")
end
;(function()
  local L0_1967
  L0_1967 = nil
  id494e5458, id494e5459, L0_1967 = LuaAuxLib.FindPicture(0, 0, 0, 0, "Attachment:领取.png", "000000", 0, 0.9)
  return L0_1967
```

Lua source recovered from a macro-scripting tool

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

The key wizard mainly uses FindPicture to find the location on the interface that needs to be input or clicked, and then automatically completes the operation.

2) The source code restored by autojs script autojs is somewhat similar to Javascript. The code is divided into two parts. Part 1 is the page layout, which describes the main interface after the tool is run:

```
"ui";
ui.layout(
    <vertical>
    <text  textColor="#B22222"  textSize="20sp"   gravity="center"   text="
    <horizontal>
    <text text="   1: 私信话术"  textColor="#9400D3"  />
    <input hint="点击此处填写"  id="we"   text="" />
    </horizontal>
    <horizontal>
    <text text="   2: 私信话术"   textColor="#9400D3" />
    <input hint="点击此处填写"   id="wr"  text=""/>
    </horizontal>
    <horizontal>
    <text text="   3: 私信话术"   textColor="#9400D3" />
    <input hint="点击此处填写"   id="wt"  text=""/>
    </horizontal>
    <horizontal>
    <text text="   4: 私信话术"   textColor="#9400D3" />
    <input hint="点击此处填写"   id="wn"  text=""/>
    </horizontal>
    <horizontal>
    <text text="   5: 私信话术"   textColor="#9400D3" />
    <input hint="点击此处填写"   id="wm"  text=""/>
    </horizontal>
    <horizontal>
    <text text="  6:喜欢用户配对"   textColor="#00008B"     margin="2"/>
```

Recovered autojs layout code

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

Part 2 is the function function, which is the operation performed after clicking a certain function:

```
var a=className("android.widget.TextView").depth(11).text("聊天").findOne()
click(a.bounds().centerX(),a.bounds().centerY())
sleep(2500)
var b=className("android.widget.FrameLayout").depth(16).drawingOrder(1).find()
var c=b.length-1
swipe(b[4].bounds().centerX(),b[4].bounds().centerY(),b[2].bounds().centerX(),b[2].bounds().centerY(),2000)
sleep(2500)
var n=ui.ww.getText()
for(var i=0;i<8;i++){
var tv=b[0]
if(tv){
    var o=i+1
    sleep(2000)
    toast("回复第"+o+"个用户")
    sleep(3000)
    var r=className("android.widget.LinearLayout").depth(15).findOne()
    click(r.bounds().centerX(),r.bounds().centerY())
    sleep(2500)
    var A=ui.we.getText()
    var B=ui.wr.getText()
    var C=ui.wt.getText()
    var D=ui.wn.getText()
    var E=ui.wm.getText()
    sleep(random(2000, 3500))
    var data = []
```

Recovered autojs function code

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

Compared with the button sprite, autojs locates the operation object by positioning the control by className.

Whether it is the button wizard or autojs, they are executed step by step according to the script code. The operation process is very fixed (you can see that the sleep time after each step of

operation is also fixed), and normal people obviously will not do such operations, so the human-computer recognition features of the tool can be extracted based on this.

3) XPosed program The source code restored by the XPosed program is the Java code of the Hook class. The code snippet is as follows:

```
public final class M implements IXposedHookLoadPackage {
    public M() {
        super();
    }

    public final void handleLoadPackage(XC_LoadPackage$LoadPackageParam arg10) {
        if(arg10.packageName.startsWith("com[redacted])) {
            d v0 = new d();
            ClassLoader v1 = arg10.classLoader;
            int v4 = 2;
            Object[] v5 = new Object[v4];
            v5[0] = Integer.TYPE;
            v5[1] = new com.DyMjsUopenpb.XTS.a.d$10(v0);
            XposedHelpers.findAndHookMethod("android.app.ApplicationPackageManager", v1, "getInstalledApplications", v5
            v5 = new Object[v4];
            v5[0] = Integer.TYPE;
            v5[1] = new com.DyMjsUopenpb.XTS.a.d$11(v0);
            XposedHelpers.findAndHookMethod("android.app.ApplicationPackageManager", v1, "getInstalledPackages", v5);
            v5 = new Object[v4];
            v5[0] = Integer.TYPE;
            v5[1] = new com.DyMjsUopenpb.XTS.a.d$12(v0);
            XposedHelpers.findAndHookMethod("android.app.ActivityManager", v1, "getRunningServices", v5);
            v5 = new Object[v4];
            v5[0] = Integer.TYPE;
            v5[1] = new com.DyMjsUopenpb.XTS.a.d$2(v0);
            XposedHelpers.findAndHookMethod("android.app.ActivityManager", v1, "getRunningTasks", v5);
```

Recovered Xposed hook code

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

The XPosed program first locates the target App through the package name, and then calls findAndHookMethod to complete the Hook of some key functions of the target App, thereby intercepting information or implanting behaviors.

If you search for the package name of your own application in the source code, you can basically determine that the target of the tool is your own business. Next, search for "findAndHookMethod" or "hookAllMethods" to see which functions are hooked by the tool and the operations performed after hooking.

1.3 Frequently asked questions and answers about tool samples

1.3.1 Why are there some samples that look the same?

Some tool samples are updated very frequently, even several versions a day. These different versions look basically the same, but you don’t need to analyze each one. Just analyze and find the latest sample (the latest version).



Tool sample record: found and analysed dates

Source: Threat Hunter original report, page 93. Original image retained.

1.3.2 Why is there a long time between the discovery time of some tool samples and the completion time of analysis?

Discovery means that we perceive the existence of this tool from intelligence, and then we need to dig out download channels and download tool samples, and then schedule an automated analysis platform to identify and analyze the tool samples. This may take a long time. The entire process is still being optimized, and the time will continue to be shortened.

2. Tool analysis and cases

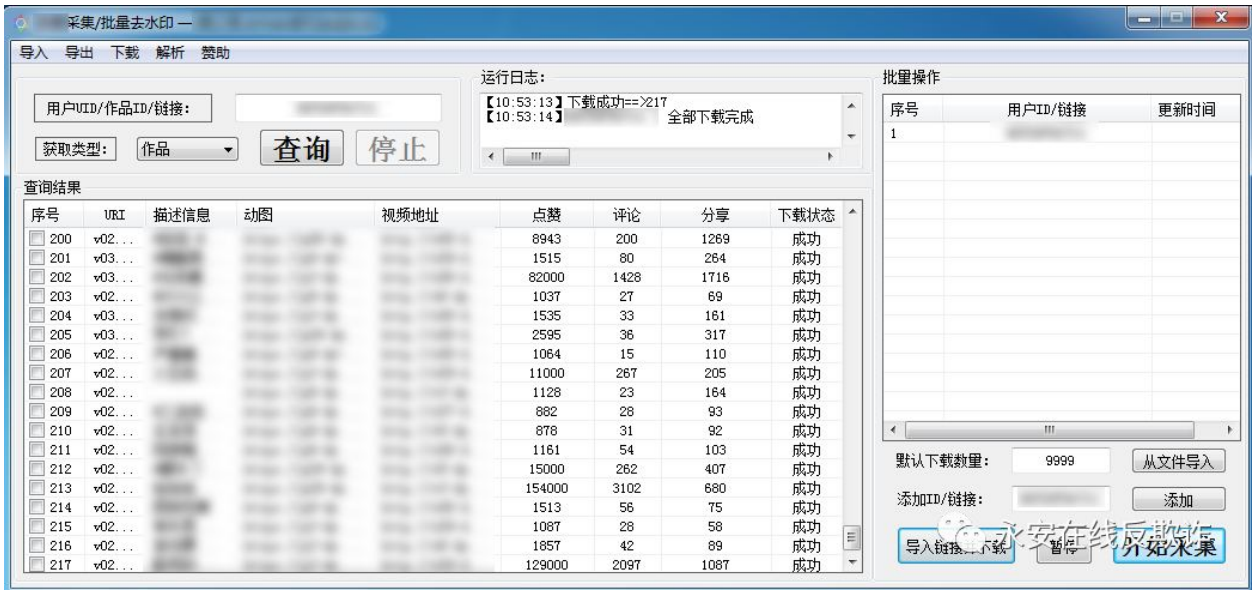
Next, we use three tools: malicious crawlers, coupon grabbing tools and registration machines to talk about the analysis methods of threat actors tool intelligence, and give corresponding case analysis:

2.1 Malicious crawler tools

2.1.1 Analysis method

Crawler tool: xx collection/batch watermark removal.exe

Tool users: ordinary users who need to download content from a short video platform in batches, as well as video reprinters and movers who need to submit videos to other platforms.



A video collection and watermark-removal tool

Source: Threat Hunter original report, page 94. Original image retained.

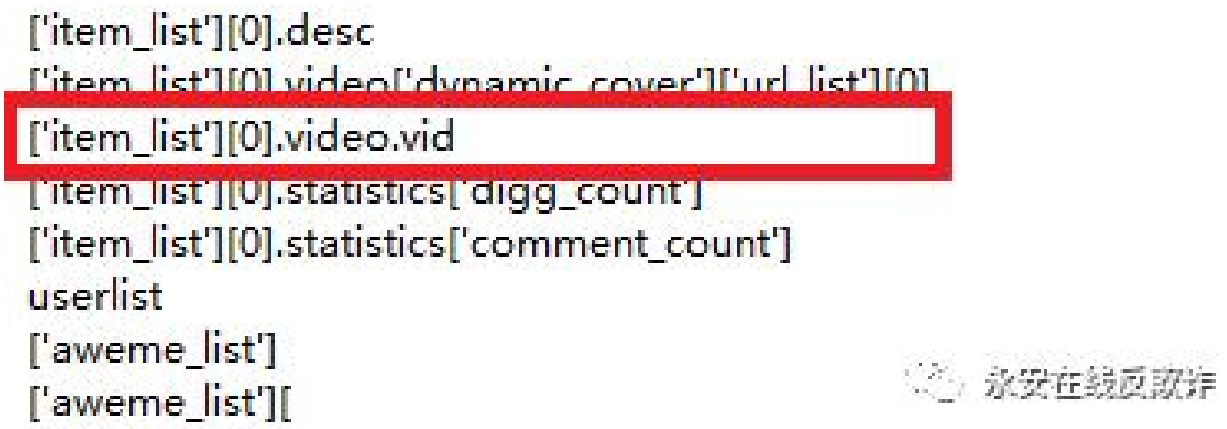
xx video collection/batch removal of watermark tool screenshot tool attack method: After entering the ID or work link of the author of the platform in the input box, crawl the works published and liked by the author and download them locally. In addition to batch downloading, videos with specified work IDs or shared links can also be collected.



Tool option for collecting an author's posts or likes

Source: Threat Hunter original report, page 94. Original image retained.

Tool analysis: This is a protocol tool running on the PC. It was discovered on May 2, 2020. This tool's malicious activity method is to obtain the unique identification ID of the video platform user by accessing the work sharing link, and then use the splicing parameters to pretend to be the mobile client of the video application to obtain the video list and video ID, and use an exposed interface to construct a watermark-free video download link to achieve the video "watermark removal" function.



Video ID obtained by splicing parameters

Source: Threat Hunter original report, page 94. Original image retained.

Video ID obtained through splicing parameters

```
.text:00406E39                  cmp     ecx, 0Ah
.text:00406E3C                  jg      loc_407078
.text:00406E42                  push    offset aLine0Ratio540p ; "&line=0&ratio=540p&media_type=4&vr_type"...
.text:00406E47                  mov     ebx, [ebp+arg_0]
.text:00406E4A                  push    dword ptr [ebx] ; video_id
.text:00406E4C                  push    offset aHttpsAweme_sns ; "https://[redacted]/play/"...
.text:00406E51                  mov     ecx, 3
.text:00406E56                  call    my_strcat
.text:00406E5B                  add     esp, 0Ch
.text:00406E5E                  mov     [ebp+lpMem], eax
```

Splicing the video ID in the tool's code

Source: Threat Hunter original report, page 95. Original image retained.



Video download addresses collected in bulk

Source: Threat Hunter original report, page 95. Original image retained.

Suggestions on attack and defense for using video IDs in the code to splice the video download addresses obtained in batches: Since users have a strong demand for crawling videos on various platforms, similar tools have been springing up like mushrooms after a rain. In this case, the platform can use threat actors tool intelligence to promptly follow up on existing threat actors crawler attacks and respond to them, and take business restriction measures on relevant business interfaces to counter attacks by threat actors.

2.1.2 Case: E-commerce crawler

Keywords: e-commerce crawler Price crawler Discovery time: May 2020 1) Comprehensive e-commerce product selection tool The tool analyzed in this analysis is a tool for "merchants without supply sources" to select e-commerce products and steal product information.

Merchants without supply, as the name suggests, are e-commerce merchants who do not need to prepare their own supply. The supply comes from products from other stores, which are repriced and sold in their own stores. When customers place an order in their own store, they use software to place an order in the corresponding store, and then earn the price difference of the goods. Product selection means that these merchants without supply sources will crawl product information from the e-commerce platform, list them, select suitable products, and add them to their stores.

This tool is a comprehensive e-commerce product selection tool with many functions, including crawler tools, link transfer tools and loading tools. Among them, the crawler tool has the greatest impact on the e-commerce platform. We have detected that this tool will crawl the product information of many e-commerce platforms including □precious, PIN□□, etc., and involves crawling the rebate ratio of the corresponding platform rebate alliance.

According to the analysis of the video tutorial of this tool, we can learn that the data crawled by this tool includes product ID, store ID, product title, product price, sales volume, commission ratio, as well as store product quantity, sales volume and other information.



Crawling product information from a keyword list

Source: Threat Hunter original report, page 96. Original image retained.



Crawling store information

Source: Threat Hunter original report, page 96. Original image retained.

Use this tool to crawl store information based on the keyword database. With the upgrade of the crawling tool, the tool has gradually added a large number of auxiliary tools in the version update, such as fission title generation, peer analysis, integrated link transfer and loading operations, etc. These new functions are all based on analysis after crawling product information, further increasing the crawler pressure on the e-commerce platform.



Competitor-analysis functions

Source: Threat Hunter original report, page 97. Original image retained.

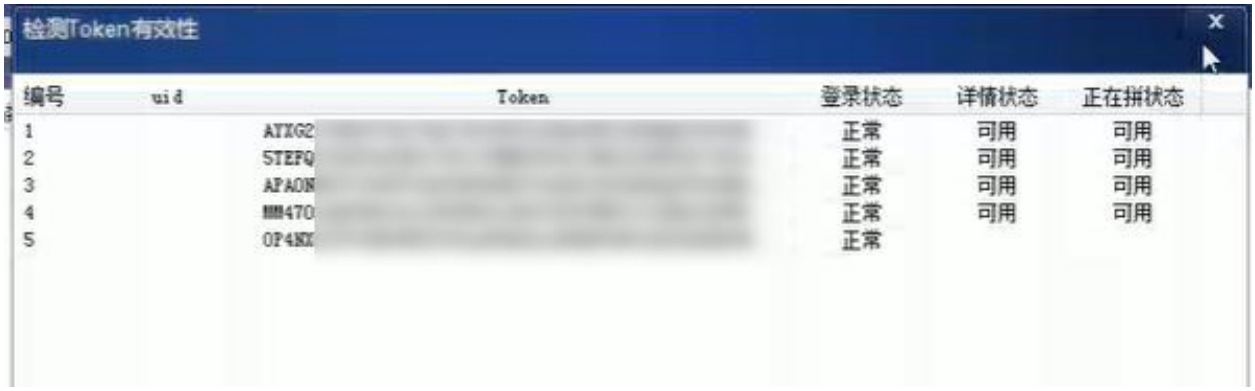
Peer analysis-related functions As we all know, major e-commerce platforms have certain countermeasures against price crawling, including but not limited to limiting the frequency of search requests for a single IP and a single account. In this tool, we can see from the main interface that in order to crawl product information, the tool adopts the "crowd tactics", that is, using a large number of account resources and agent IP resources to perform "distributed crawling" of data, crawling the required store ID, product ID, title, price and other data, and then integrating it into a list, thereby crawling a large amount of product information locally. The main e-commerce platforms crawled by this tool are □precious and □□.



Crawling product information from an e-commerce platform

Source: Threat Hunter original report, page 97. Original image retained.

The picture shows crawling Pin 00 product information. When crawling, the tool will use the software integrated agent IP and the pre-imported e-commerce platform account to crawl. Since the e-commerce platform will conduct behavioral verification or blocking of accounts with abnormal behavior, in order to improve the efficiency of crawling, this tool will also detect the availability of the account login information Token.



Account and token checks in the crawler

Source: Threat Hunter original report, page 98. Original image retained.

2) Basic information of tool analysis:

File name	**smart-product-picker.exe
File MD5	07cd03571**********b480576e
File size	30.64M
Discovered	May 2020
Language	Easy Language
Packer	VMP
Platform	Windows

Basic information on the e-commerce crawler

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

Detailed analysis:

This tool was first discovered on May 26, 2020. It is a tool software written in E language and packed with VMP.

Through static analysis of the tool, we can confirm that the tool is a protocol tool that can automatically crawl product information by cracking the business interface communication protocols of major e-commerce platform apps and sending carefully forged data packets to the e-commerce backend servers.

Compared with simulated button scripts (touch wizard/button wizard, etc.), protocol tools are free from device limitations. cybercriminal groups use protocol tools to complete batch and large-scale crimes at a lower cost, so the harm is more serious.

Take the tool's crawling of product information on Pin00 as an example. The tool will first call the following interface to log in:

hxxps://mms.pin***.com/latitude/auth/login

```
v48 = (int *)"https://mms.pir      .com/latitude/auth/login";
if ( v72 )
  sub_A7015F(v72);
v72 = v48;
v64 = (char *)sub_86CC04();
v63 = 0;
v48 = 0;
v62 = "crawlerInfo";
(*(void (__stdcall **)(int **, char **, char **, _DWORD, _DWORD))(*v71 + 20))(&v71, &v62, &v64, 0, 0);
if ( v62 )
  sub_A7015F(v62);
if ( v64 )
  sub_A7015F(v64);
v64 = 0;
v48 = 0;
v63 = "oppo a33";
v62 = "deviceName";
(*(void (__stdcall **)(int **, char **, const char **, _DWORD, _DWORD))(*v71 + 20))(&v71, &v62, &v63, 0, 0);
if ( v62 )
  sub_A7015F(v62);
```

Crawler code calling the login interface

Source: Threat Hunter original report, page 99. Original image retained.

Some interfaces used when crawling product information:

hxxps://mms.pin*.com/venus/api/goods/listhxxps://pifa.pin*.com/pifa/goods/queryGoodsDetailhxxps://pifa.pin*.com/pifa/goods/queryGoodsPropertyInfohxxps://youhui.pin*.com/network/api/goo ds/queryByGoodsIdhxxps://mms.pin*.com/vodka/v2/mms/query/display/mall/goodsListhxxps://mms.pin*.com/sydney/api/mallScore/queryMallScoreInfo part of the interface request code, in which the request header has been built-in. In addition, this tool also uses a CAPTCHA-solving service and an agent platform to bypass the anti-crawler strategy of the e-commerce platform.

```
v76 = "accept: */*\r\n"
      "accept-encoding: gzip, deflate, br\r\n"
      "accept-language: zh-CN,zh;q=0.9\r\n"
      "anti-content: 0aoAfxnqUMhYq9E2h48L-4pc60UC4eIJO4fGDBpl6B2kOKCEL9n1skKCoOxEIhy3OwKR-VIpMoLhVEiL9XChWSNFiAw8Hg"
      "9EQ97V1ChQ9iOKNaJZOJ5mRZ9v5KDO-8vh9h0x-CwvBEOlimhtsoeGKxpp_VvtJonpae8pctgffax-MB9srCcVL0qmCZLWi998DvQYqTAabJ"
      "UZxPzwmmYfw65Q4PfewwjYpPWoVL98ywkM0BZFgJxgAOm1Uf1teMzVdJSsqGnnpa0-jtoNugG6rRwJoD2QO_SvAHDyaOIwmC4CUuqRLnLkQ4"
      "8BkEUPlRaRQHrpTLakvvenvWbFzF0s-u2MlGwyA7HbhSPzLn_iGX1vcJTWyqzIFwVaCX_aBl_2fwoW4cY1X8p0PLTOVMuvAWc5H-hFSo8OKf"
      "cL7JReIi3dONRckqLMRMyKN-Qap_kiMD7RMNL2Ndkhsd6r21fLFvNn-dfW7cjh_0d8hGLeKYjKJhfb2rpL6hJ\r\n"
      "cache-control: max-age=0\r\n"
      "content-length: 22\r\n"
      "content-type: application/ison\r\n"
      "cookie: api_uid=                    ; _pati=TFeKtKlf8O5tf1APDi2QOygReSaH3qmB; _nano_fp=XpEoX5dJl09qlpdon"
      "o_x7ZumfjIHrzYbLDTPgQ2Q; VISITOR_PASS_ID=G0qKdjIMqg7g                    RWKZAL2BZWyP6eF2DcRxqmRplEL0BjQBfhY"
      "HTv7WGFWm815mA-ZNPwkEO862XZV_irhUejRKhuo_f41c0dbdeb\r\n"
      "origin: https://pifa.pin      .com\r\n"
      "referer: https://pifa.pin      .com/goods/detail/?gid=3404818178\r\n"
      "sec-fetch-mode: cors\r\n"
      "sec-fetch-site: same-origin\r\n"
      "user-agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safa
v75 = 0;
v74 = 0;
v73 = (int *)sub_41F983(
                &v111,
                1,
                1,
                &v109,
                1,
                &v74,
                0,
                &v75,
                0,
                &v76,
```

Request code with built-in headers

Source: Threat Hunter original report, page 99. Original image retained.

The agent platform used by this tool:

hxxp://www.**daili.cn/The CAPTCHA-solving service used by this tool:

hxxp://www.**dama.com/3) Attack and defense suggestions Crawlers have been a threat to e-commerce platforms for a long time, and tools for crawling commodity price information are also emerging in endlessly. Although various e-commerce companies already have relatively complete means to detect and intercept some abnormal automated requests, demand from the cybercrime ecosystem continues, and tools that bypass corresponding rules will naturally appear. This is a long-term offensive and defensive confrontation.

Faced with this situation that requires long-term confrontation, e-commerce platforms can adopt flexible and diverse identification and interception methods to increase the cost of cybercrime ecosystem automated tools and inhibit their data crawling. To identify abnormal crawling behaviors, detection methods such as IP risk identification, abnormally frequent account logins, abnormal account login devices, and excessive account search behavior frequency can be used for discovery and judgment. Various verification methods including but not limited to character verification codes, voice verification codes, etc. can be used to increase the bypass cost of cybercrime ecosystem, and intercept the access of threat actors without affecting the access of real users.

2.2 Coupon grabbing tool

2.2.1 Analysis method

Coupon grabbing tool: xxxx20200615.exe Tool user: This tool is mainly a special tool for specific activities on a certain platform. Its main users are threat actors who use the platform's large coupons to make profits.

Tool attack method: The main attack method of this tool is to use the platform’s interface without device verification to automatically grab coupons, and use a large number of accounts to obtain a large number of coupons for profit.

Tool analysis: This tool appeared on June 15, 2020, and is written in QT language. Through static reverse analysis of the tool code, its main functions were discovered:

```
if ( *(_DWORD *)v304 < 0xFFFFFFFF && *(_DWORD *)v304 != 0 )
  _InterlockedAdd((volatile signed __int32 *)v304, 1u);
((void (__fastcall *)(int *, int))ZN7QString6appendERKS_)(&v306, v153);
sub_43FBB0((int)&v307, (int)&v306, "优惠券领取");
v154 = v307;
v308 = v307;
                        . .
{
  sub_43DAB0(&v216);
}
v366 = (volatile signed __int32 *)((int (__stdcall *)(const char *, signed
                                   "优惠券已领过",
                                   18);
v88 = ZNK7QString7indexOfERKS_iN2Qt15CaseSensitivityE(&v273);
sub_43DFB0(&v366);
  v286 = ((int (__stdcall *)(const char *, signed int, volatile signed __int32 **))Z
           "优惠券已抢完",
           18,
           v191);
  if ( ZNK7QString7indexOfERKS_iN2Qt15CaseSensitivityE(&v273) == -1 )
  {
    v287 = ((int (__stdcall *)(const char *, signed int, int))ZN7QString16fromAscii_
             "优惠券已领完",
             18,
             v192);
    if ( ZNK7QString7indexOfERKS_iN2Qt15CaseSensitivityE(&v273) == -1 )
    {
      sub_43DF70("当前优惠不在活动期间");
```

永安在线反欺诈

Coupon-grabbing code

Source: Threat Hunter original report, page 101. Original image retained.

Coupon-related codes In the code of the tool, we can see that the coupons it targets include hotel coupons, ticket coupons, and air ticket coupons:

```
                1) )
          sub_43DFF0("酒店券");
      }
      else
      {
        sub_43DFF0("[]票券");
      }
    }
    else
    {
      sub_43DFF0("机票券");
    }
```

永安在线反欺诈

Coupon types targeted: hotel, ticket and flight coupons

Source: Threat Hunter original report, page 101. Original image retained.

In order to bypass the platform's fraud controls restrictions on IP addresses, the tool will also obtain IP resources on some proxy IP platforms and set up proxies before grabbing coupons. In the code, we see its hard-coded bound proxy IP account and password.



Hard-coded proxy IP platform account, password and API

Source: Threat Hunter original report, page 102. Original image retained.

Agent IP platform account password and interface attack and defense suggestions:

Faced with this kind of threat actors tool that uses proxy IP to automatically grab coupons in batches, in addition to increasing the cost of coupons from the business level and reducing the potential benefits of threat actors, it can also be defended from the perspective of the proxy IP. The risk IP profiling function of Threat Hunter can be used to intercept requests through the proxy IP or perform secondary security verification. At the same time, the tool also exposed the problem of unverified request sources in some interfaces, and relevant business security reinforcement must be carried out in the subsequent development of the coupon collection activity interface.

2.2.2 Case: Tug-of-war between threat actors in marketing campaign scenario

Keywords: marketing activities, threat actors attack, malicious tool discovery time: August 2020 1) malicious activity tool for a certain marketing activity Super Friday is a fixed weekly marketing activity held by a domestic network operator in the "**Business Hall" app since June 2020. The initial stage of this activity was a "Come and Eat Overlord Meal" activity carried out by operators and takeaway platforms. The payment methods included online payment and mobile phone point redemption, which enabled free acquisition of relevant coupons. As the influence of the event gradually increased, the event was renamed "Super Friday", and the scope of snap-up purchases gradually increased to include large discount coupons for audio and video website members, travel, and physical beverage stores.



The campaign at launch, run with one food-delivery platform

Source: Threat Hunter original report, page 103. Original image retained.



Coupons added to the campaign later

Source: Threat Hunter original report, page 103. Original image retained.

The initial event only cooperated with one food delivery platform. Recently, various new coupons have been added. As the event heats up every week, threat actors are also ready to take action, especially the most popular takeout red envelope of "30 off for purchases over 10 yuan", which has stimulated threat actors' interest in this event, and corresponding snap-up tools have also "emerged at the historic moment." However, the "real hammer" that truly detected the large-scale malicious activities of threat actors was that during an event at the end of September, many threat-actor tools had too many accesses to the activity interface.

Unable to respond normally, a large number of threat actors were unable to perform payment operations after placing orders, resulting in payment timeouts and rush orders being released. The promotion-abuse actors made large-scale complaints in the communication community around various problems existing in the event, which also confirmed that the event has been paid attention to and attacked by a large number of people.



Promotion abusers complaining after the system was overloaded

Source: Threat Hunter original report, page 104. Original image retained.

But having said that, it is quite common for people to be unable to place orders due to panic buying of tools. This is the first time we have heard of the system being paralyzed and unable to pay due to panic buying of tools. This is the first time we have heard of threat actors having to go to customer service to complain. As for why this snap-up tool can slow down the response speed of the payment business, we might as well directly use the expert tool analysis function of the Karma business intelligence search engine to analyze the malicious methods.

2) Basic information of tool analysis:

File name	***Friday***-30 coupon v1.52.exe
File MD5	7a87c9efcd0e**********e3155e418c
File size	744,448 bytes
Discovered	2020/08/29 23:01:38
Language	Easy Language
Packer	UPX
Platform	Windows

Basic information on the coupon-grabbing tool

Source: Threat Hunter original report, page 104. Original figure with Chinese text replaced by English.

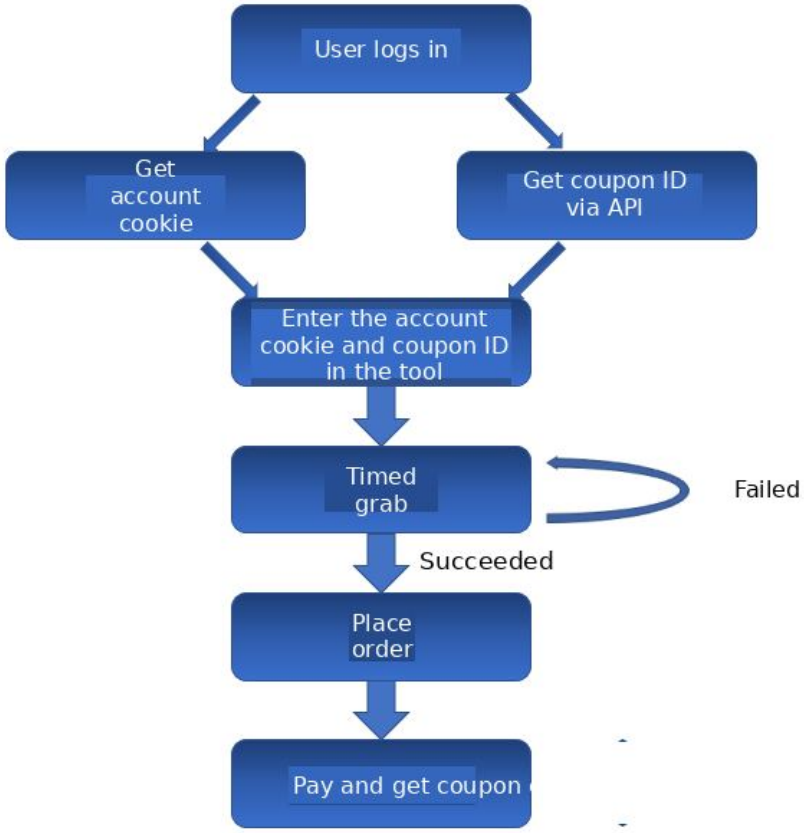
Interface after running the program:



The coupon-grabbing tool after launch

Source: Threat Hunter original report, page 105. Original image retained.

The operation flow chart of the program is as follows:



How the coupon-grabbing tool works

Source: Threat Hunter original report, page 105. Original figure with Chinese text replaced by English.

Detailed analysis:

This tool was first discovered on August 29, 2020. It is a tool software written in E language and packed with upx.

After performing static analysis on the tool after unpacking, we can confirm that the tool is a protocol tool. By cracking the "** business

It uses the business interface communication protocol of the "hall" app to send carefully forged data packets to the backend server of the application, thereby achieving the purpose of automating the purchase of coupons in batches.

Compared with simulated button scripts (touch wizard/button wizard, etc.), protocol tools are free from device limitations. cybercriminal groups use protocol tools to complete batch and large-scale crimes at a lower cost, so the harm is more serious.

```
v5 = "D&version=android%405.91&keyVersion=";
v18 = (LPVOID)sub_4010DB((unsigned int)"mobile=");
if ( lpMem )
  sub_414DC4(lpMem);
v17 = 0;
v16 = 0;
v15 = 0;
v14 = 0;
v13 = 0;
v12 = 0;
v11 = 0;
v10 = 0;
v9 = 0;
v8 = "https://m.client.[redacted]/mobileService/sendRadomNum.htm";
v7 = (LPVOID)sub_4089B0(
               &v8,
```

Code that grabs coupons with three accounts' cookies

Source: Threat Hunter original report, page 106. Original image retained.

The tool first calls the interface:

https://m.client.100**.com/mobileService/sendRadomNum.htm

- https://m.client.100**.com/mobileService/radomLogin.htm Send a request to obtain a verification code. After filling in the verification code, send a login request to obtain the cookie corresponding to the phone number. Then use the phone number corresponding to this cookie to grab coupons. This software supports the use of cookies with 3 numbers to grab coupons. Some of its code snippets are as follows:

```
v26 = (LPVOID)sub_4010DB((unsigned int)"isRemberPwd=false&loginStyle=0&deviceId=");
if ( lpMem )
  sub_414DC4(lpMem);
if ( v28 )
  sub_414DC4(v28);
if ( v27 )
  sub_414DC4(v27);
v25 = 0;
v7 = 0;
v24 = 0;
v23 = 0;
v5 = (_DWORD *)sub_414DBE(8u);
v22 = v5;
*v5 = 0;
v5[1] = 0;
v21 = 0;
v20 = 0;
v19 = 0;
v18 = 0;
v17 = 0;
v16 = 0;
v15 = 0;
v14 = 0;
v13 = 0;
v12 = "Content-Type: application/x-www-form-urlencoded\r\nHost: m.client.[redacted]\r\nUser-Agent: okhttp/3.9.1";
v11 = 0;
v10 = "https://m.client.[redacted]/mobileService/radomLogin.htm";
v9 = (LPVOID)sub_4034E0(
               &v10,
```

Code that sends the login verification request

Source: Threat Hunter original report, page 106. Original image retained.

Next, the software uses the following interface to obtain coupon information:

https://m.client.100**.com/welfare-mall-front-activity/mobile/activity/get619Activity/v1?

whetherFriday=YES&from=955000006 Some of its code snippets are as follows:

```
v35 = "User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 14_0_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mo"
      "bile/15E148 [illegible]version:iphone_c@7.0500}{systemVersion:dis}{yw_code:}";
v34 = 0;
v33 = 0;
v32 = 0;
lpMem = "https://m.client.[illegible]/welfare-mall-front-activity/mobile/activity/get619Activity/v1?whetherFriday=YES&from=955000006";
v30 = (LPVOID)sub_40B7A5(
                (int)&lpMem,
```

Code that fetches coupon information

Source: Threat Hunter original report, page 107. Original image retained.

After obtaining the coupon information, the user can start using the tool to purchase coupons. The interface used is:

https://m.client.100**.com/welfare-mall-front/mobile/api/bj2402/v1 Some code snippets are as follows:

```
.text:0040F70D                  mov     [ebp+var_C], eax
.text:0040F710                  push    offset asc_4D5BF2 ; ":开始自动线程抢卷!(活动是每周五开始)"
.text:0040F715                  push    [ebp+var_C]
.text:0040F718                  push    offset asc_4D4E32 ; ":"
.text:0040F71D                  push    [ebp+var_8]
.text:0040F720                  push    offset asc_4D4E32 ; ":"
.text:0040F725                  push    [ebp+lpMem]
.text:0040F728                  push    offset asc_4D5C17 ; "已启动定时抢卷,将在"
.text:0040F72D                  mov     ecx, 7
.text:0040F732                  call    sub_4010DB
.text:0040F737                  add     esp, 1Ch
```

Code that loops to grab coupons

Source: Threat Hunter original report, page 107. Original image retained.

Codes related to loop coupon grabbing

```
while ( 1 )
{
  v20 = (LPVOID)sub_414DB8(4);
  if ( v20 != (LPVOID)-1 )
    break;
  lpMem = (LPVOID)sub_4010DB((unsigned int)"reqdata=%7B%22goodsId%22%3A%22");
  v20 = (LPVOID)sub_414DDC(1375797249, (LPCSTR)0x16012D10, 8, -1);
  v19 = 0;
  v18 = 0;
  v17 = 0;
  v16 = 0;
  v15 = 0;
  v14 = 0;
  v13 = 0;
  v12 = 0;
  v11 = 0;
  v10 = 0;
  v9 = 0;
  v8 = 0;
  v7 = 0;
  v6 = 0;
  v5 = "User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 14_0_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) M"
       "obile/15E148 [illegible]{version:iphone_c@7.0500}{systemVersion:dis}{yw_code:}";
  v4 = 0;
  v3 = "https://m.client.[illegible]/welfare-mall-front/mobile/api/bj2402/v1";
  v2 = (LPVOID)sub_40B7A5(
                 (int)&v3,
```

Coupon-ordering code

Source: Threat Hunter original report, page 108. Original image retained.

After grabbing it, go to app-My Orders-Points Order to pay.

Based on the above analysis, this tool software is a typical "scalper" software that seizes the resources of ordinary users, causing the product discounts provided by operators to ordinary users to be illegally obtained by a small number of scalpers, destroying the market order of integrity and fair transactions.

Version change differences:

This malicious activity tool was first discovered on August 29. In the Karma business intelligence search engine, we found that this tool has undergone multiple version iterations. Each iteration lowers the threshold for threat actors to use the tool, expands the influence of the tool, and then affects more and more threat actors to start using the tool to conduct malicious activity.

Version	Found	Features
V1.0	Aug 29	No code sending or login to get cookies (users had to capture cookies themselves with a packet sniffer); no timed grabs; no restock sniping
V1.1	Sep 3	Code sending and login to get cookies supported
V1.3	Sep 4	Timed grabs and restock sniping supported
V1.4	Sep 18	From V1.3 on, the tool can grab coupons once an account is logged in; later upgrades add no new front-end features
V1.5	Oct 1	
V1.51	Oct 2	
V1.52	Oct 6	

Versions of the coupon-grabbing tool

Source: Threat Hunter original report, page 108. Table re-typeset in English from the original.

Comparison between versions of this tool

3) cybercrime ecosystem costs and profits: threat actors need to pay the corresponding points or amount after a successful purchase, and the cost is 10 yuan. In terms of resale of coupon codes, the resale price is generally 20% off the listed price of the coupon code, that is, the selling price of a 30 yuan coupon code is about 24 yuan, and the profit after removing the cost is about 14 yuan.

Cost: Pay 10 yuan after successful purchase.

Profit: The coupon code is sold for 24 yuan, and the profit is about 14 yuan.

4) Offensive and defensive suggestions: This tool will periodically access the company's https://m.client.100**.com/welfare-mall-front/mobile/api/bj2402/v1 interface, and the values of some request headers are hard-coded in the code. Therefore, the company can distinguish whether it is an automated tool or a request initiated by a normal user based on the characteristics of "whether the interface is accessed regularly and multiple account request header values are the same".

From the perspective of business availability, since the activity interface calls m.client.100**.com, the unified interface source of the application, excessive number of access requests for this domain name will cause a chain reaction and seriously affect the experience of other users. You

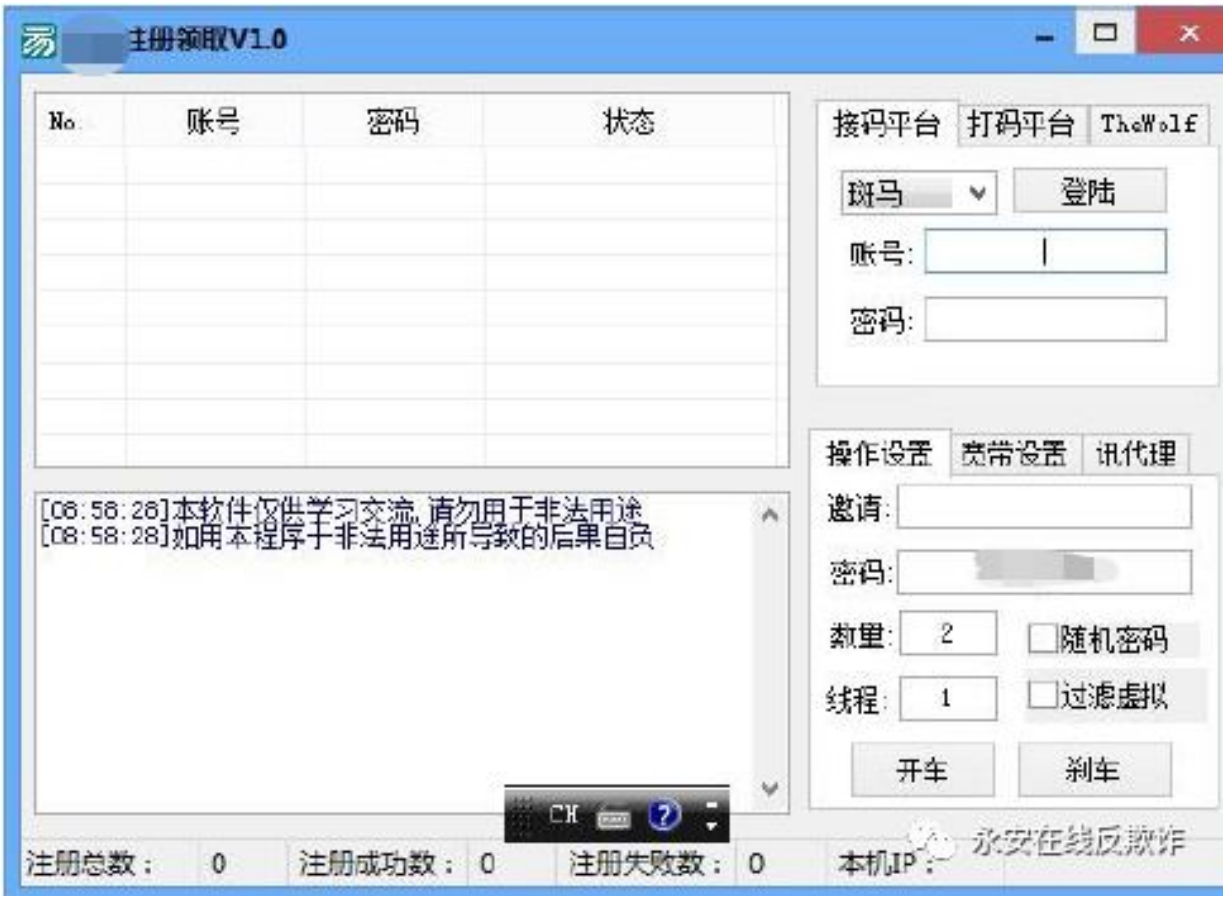
can split the request interface into an activity-specific interface to avoid chain reactions and affect the operation of other businesses in the application.

2.3 Registration machine tool

2.3.1 Analysis method

Registration machine tool: xx Register and receive V1.0.exe tool users: Users who use this tool are mainly threat actors who focus on malicious registration and redemption of coupons.

Tool attack method: This is a cybercrime ecosystem special tool that runs on a PC. It directly cracks and forges the communication protocol between the app and the server to automate login, registration and other operations. Compared with simulated keystroke scripts, protocol tools are free from device limitations. threat actors can complete batch and large-scale crimes at a lower cost, so the harm is more serious.



A registration and coupon-claiming tool

Source: Threat Hunter original report, page 110. Original image retained.

Analysis of xx registration and collection tool screenshot tool:

During the login process of the tool, two interfaces were constructed and accessed. These two interfaces follow the https protocol and the request method is POST. By capturing packets and analyzing the e-commerce app, threat actors can easily obtain relevant information and then forge the interface protocols and parameters. Through reverse analysis, we found that the tool obtained the phone number through the SMS verification-code receiving service, and then obtained the verification code to log in directly.

platform	android	hardcode
appId		hardcode
channel		hardcode
v	4.37.6	hardcode
loginToken	""	hardcode
deviceTrait	RMX1931	hardcode
timestamp		Dynamic
iid	""	Empty
oaid	""	Empty

Parameters of one interface: mostly hard-coded

Source: Threat Hunter original report, page 110. Original figure with Chinese text replaced by English.

Suggestions for attack and defense of parameter list of an interface:

Most of the interface parameters extracted from the assembly code of the tool are hardcoded, so the platform can identify registration requests initiated by the tool based on these hardcoded parameters as features.

At the same time, in this tool, we see the technology used by threat actors in high-net-worth malicious registration attacks: the registration machine no longer only has a single registration function, but now also integrates an automated SMS verification-code receiving service and a built-in network module, using broadband dial-up and proxy IP to multi-thread to bypass the platform's business security fraud-control system. threat actors use complex attack methods, which makes the existing registration fraud controls links at risk of being bypassed. At this time, the platform can combine risky IP portraits and risky phone number portraits to intercept the process of threat actors registering fake accounts in batches, or impose business-level restrictions on relevant accounts during the login process to avoid losses.

2.3.2 Case: "Shoe chasers" who make profits by collecting shoe cards

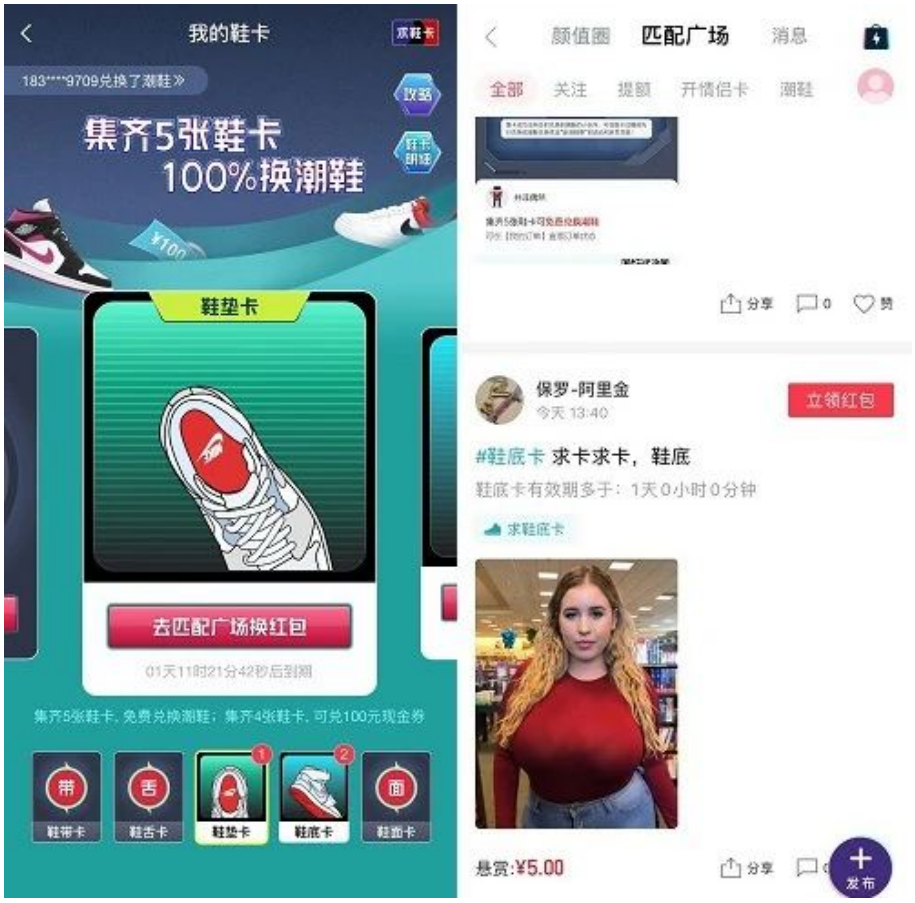
Keywords: e-commerce promotion-abuse purchasing, malicious registration Discovery time: September 2020 1) Automated exchange tool A certain financial application launched a "collect shoe cards for trendy shoes" activity in order to stimulate user growth. Users can obtain "shoe cards" by participating in the activity and completing activity tasks. After users collect the shoe cards, they can choose their favorite trendy shoes to redeem. However, due to the limited types and quantities of trendy shoes released by the event at different times, and the high demand for some relatively high-value trendy shoes, it is necessary to use a "rush purchase" method to redeem trendy shoes. Shortly after the event was launched, the Threat Hunter business risk perception platform discovered a tool for the event, which could automate the process of redeeming trendy shoes.



An online earning platform promoting the shoe-card campaign

Source: Threat Hunter original report, page 111. Original image retained.

An introduction to the activity on an online earning platform



Inside the app: collect five shoe cards to swap for sneakers

Source: Threat Hunter original report, page 111. Original image retained.

In-app screenshot 2) The promotion-abuse workflow uses a large number of accounts to receive shoe cards, and conducts certain card transactions in the matching square to collect shoe cards. After collecting the shoe cards, use the snap-up tool to snap up relatively high-value shoes and then sell them on other platforms.



Collecting a full set of shoe cards

Source: Threat Hunter original report, page 112. Original figure with Chinese text replaced by English.



Grab-and-resell flow

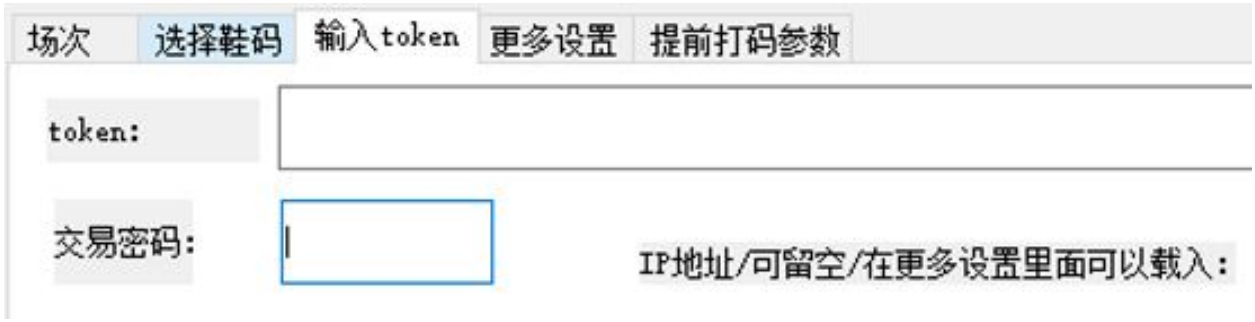
Source: Threat Hunter original report, page 112. Original figure with Chinese text replaced by English.

3) The screenshot of tool analysis software running is as follows:



Tool settings: sneaker redemption

Source: Threat Hunter original report, page 113. Original image retained.



Tool settings: accounts

Source: Threat Hunter original report, page 113. Original image retained.



Tool settings: threat-actor resources

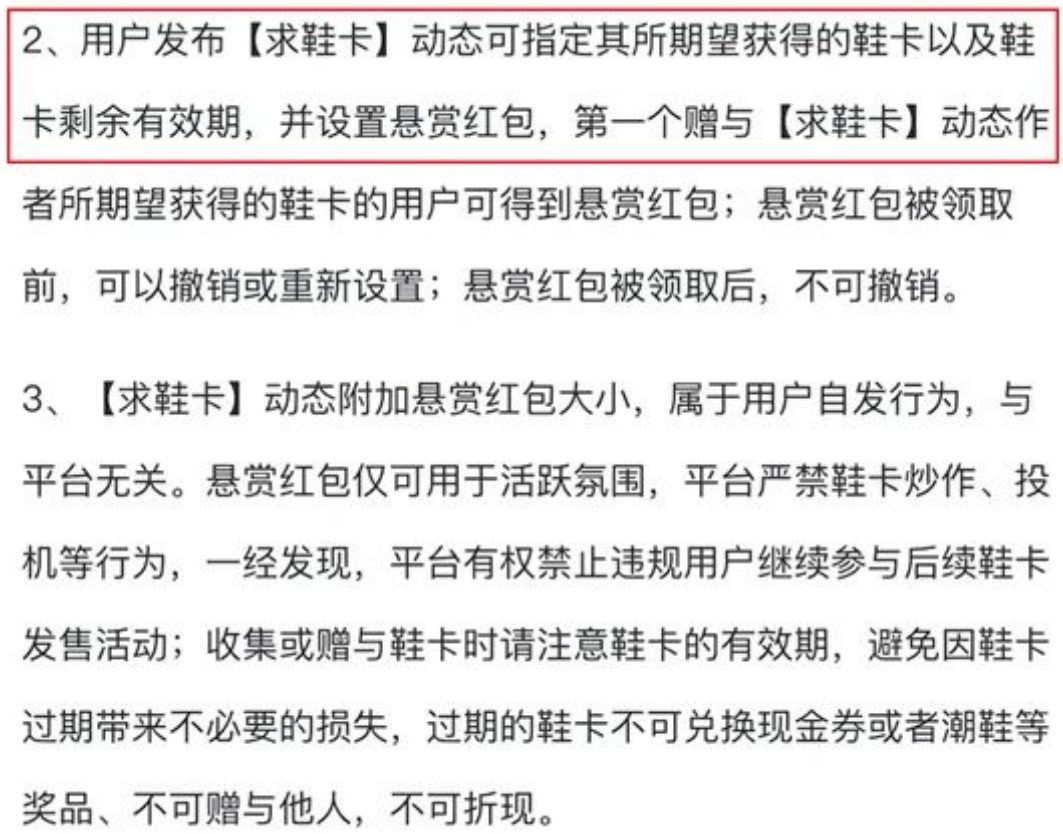
Source: Threat Hunter original report, page 113. Original image retained.

Trendy shoe redemption information configuration account configuration cybercrime ecosystem related resource configuration target interface of the attack:

https://api.***.com/v2/card/exchange/checkShare

- https://api.***.com/v2/card/exchange/confirm
- https://api.***.com/v2/card/exchange/skuInfo
- https://api.***.com/v2/order/address/all.json
- https://api.***.com/v2/shoes/card/sessionList

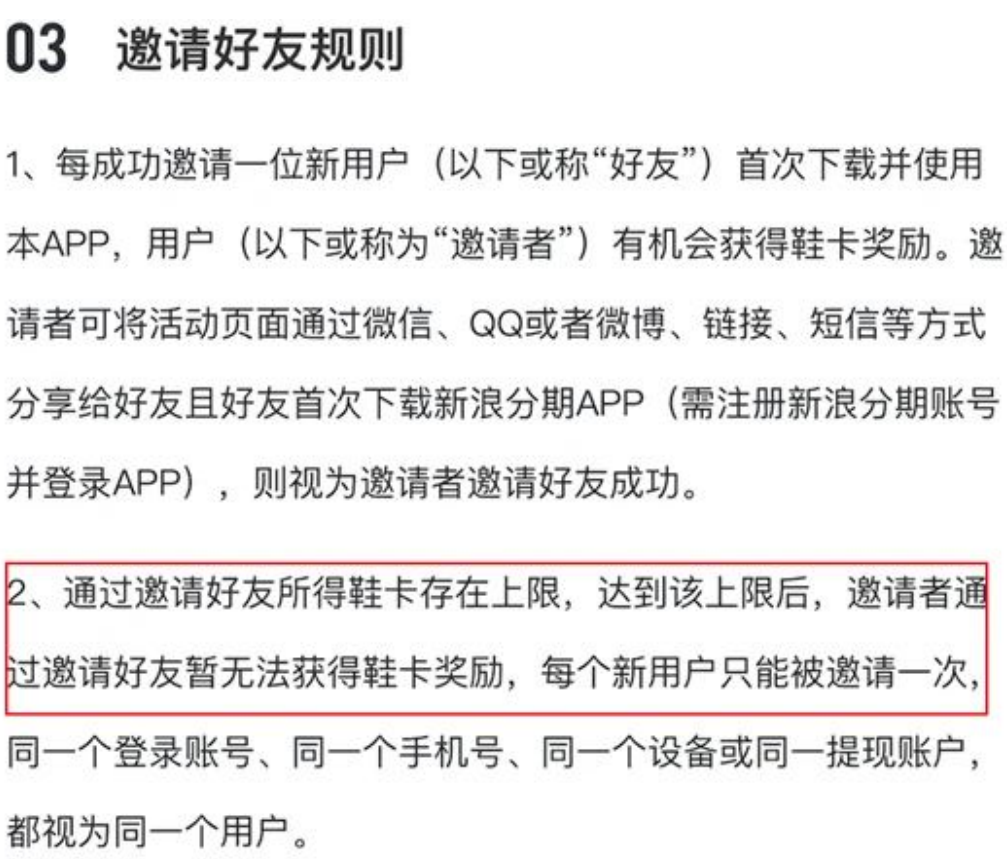
This is a PC-side protocol tool. You need to prepare the account token and transaction password of the shoe card in advance. The shoe card can be obtained through "reward red envelopes".



Campaign rules on shoe-card bounties

Source: Threat Hunter original report, page 114. Original image retained.

You can also use the SMS verification-code receiving service to invite new users to obtain shoe cards, but there is an upper limit on the number of new users you can invite to obtain shoe cards, so it is difficult to collect all the shoe cards through this method.



Campaign rules on inviting friends

Source: Threat Hunter original report, page 114. Original image retained.

This tool has two built-in proxy platforms, which are used to bypass the platform's fraud-control strategy for IP.

hxxp://www.*daili.cn/hxxp://www.****daili.com/ also has a built-in CAPTCHA-solving service for bypassing verification codes.

https://captcha.**studio.cn/4) cybercrime ecosystem Cost and Profit cybercrime ecosystem grabs high-value trendy shoes and then sells the trendy shoes to make a profit.

Cost: The cost of collecting shoe cards is 200~400 yuan. Profit: Selling trendy shoes is 500~5,000 yuan. 5) Attack and defense suggestions For this kind of tool that uses multiple accounts and uses proxy IP, verification code coding, etc. to bypass platform fraud controls, from the business level, we can use risk IP portraits to pay attention to the proxy tags of relevant IPs. At the same time, we can also judge whether the user behavior of the account is abnormal by crossing the login IP area of □□the relevant account, and determine whether the account is held by threat actors.

In addition to solutions for business fraud controls, since the prizes are physical commodities, they can be handled more stringently in terms of logistics and award issuance processes. For concentrated large-scale prize redemption activities in similar areas, methods such as manual prize distribution, delayed prize distribution, and human-operated information verification can be adopted to avoid losses.

Description

1. Data source description:

The data in this report comes from Threat Hunter's Karma business intelligence search engine. It is sampled and analyzed based on the data monitored on Karma. There may be certain deviations between the obtained data analysis results and the actual situation. Please understand.

2. Description of business intelligence monitoring platform:

Karma, a business intelligence monitoring platform, takes an attacker's perspective and relies on powerful cybercrime ecosystem control capabilities and in-depth intelligence processing capabilities to help enterprises accurately screen out malicious traffic in business links, restore risk scenarios, and quantify the impact on business. It also continuously monitors threat actors in real time, drives iteration of the fraud controls decision engine, and thereby improves the overall offensive and defensive efficiency of the enterprise.