THREAT HUNTER RESEARCH

Human-Operated Fraud Industry Research Report

A study of human-in-the-loop fraud operations and why intelligence-led defense is needed alongside automated controls.

Original publication: 2020-07-15
Research team: Threat Hunter Research Team
Source report: 23 pages

Original report text

This text version is reconstructed based on the 23-page original PDF, retaining the report narrative, chapters and research scope; the cover, repeated table of contents and purely decorative pages are not repeated. Localized figures are placed in context throughout this web edition, with the original PDF retained for reference.

Directory

1. Overview and key points

2. Development and Current Situation

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

2.1.1 Involved in multiple industries

2.1.2 Multi-scenario penetration

2.1.3 Multi-task participation

2.2 Human-operated fraud apps have expanded rapidly

2.2.1 Exponential growth in app activity and downloads from 2014 to 2020 .. 9

2.2.2 Rapid growth of developers from 2014 to 2020

2.3 Profile of participants in human-operated fraud

2.3.1 Number of participants in human-operated fraud

2.3.2 Ratio of male to female cheaters

2.3.3 Age distribution of real cheaters

2.3.4 Geographic distribution of participants in human-operated fraud

2.4 Industry losses associated with human-operated fraud

3. Pain points and hazards

3.1 human-operated fraud vs. automated fraud

3.2 human-operated fraud vs traditional fraud controls

3.3 Additional risks created by human-operated fraud

4. Confrontation and Resolution

4.1 Intelligence Dimension

4.2 Data Dimension

5. Write at the end

1. Overview and key findings: human-operated fraud challenges conventional fraud controls

Human-operated fraud is malicious activity carried out by real participants to imitate legitimate user behavior, undermining platform security and business stability. 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.

The key points of this research report are as follows:

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) The human-operated fraud ecosystem has expanded rapidly. From 2014 to 2020, the human-operated fraud platform (app)

The number 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.

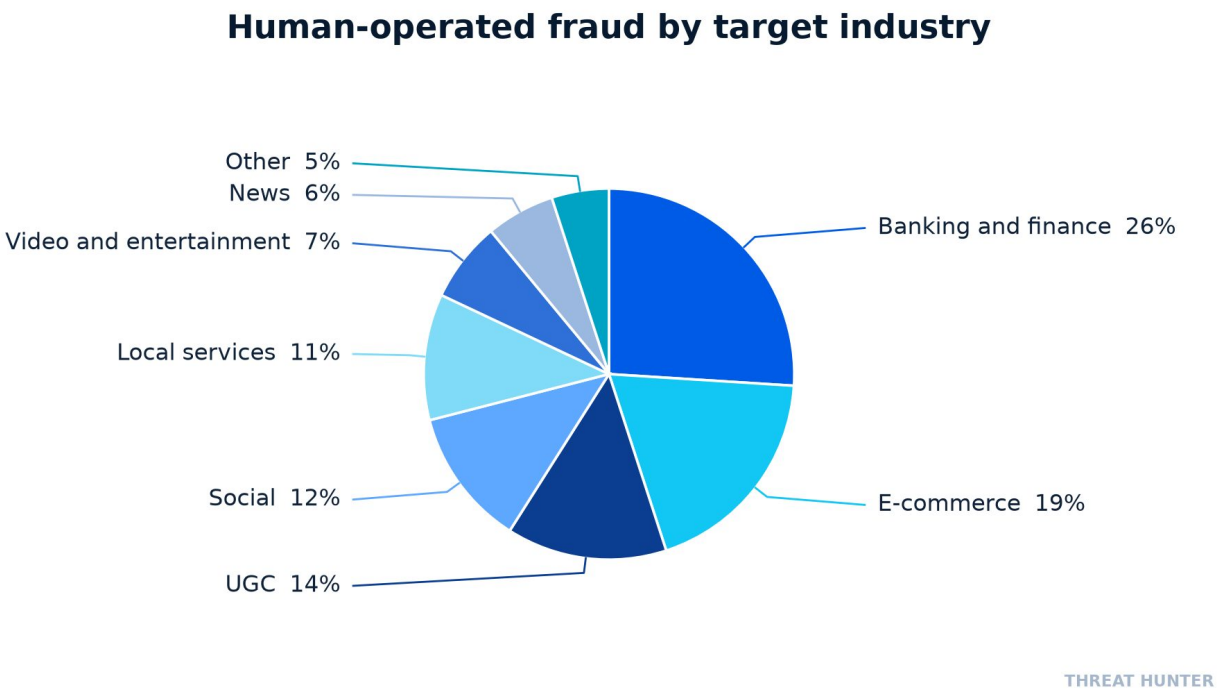
2. Development and current situation

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 diversified 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 (instant-messaging groups, voice-chat rooms, etc.) to today's platformization and fragmentation changes.

2.1 Widely penetrated into multiple industries, multiple scenarios, and multiple tasks

2.1.1 Involved in multiple industries

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



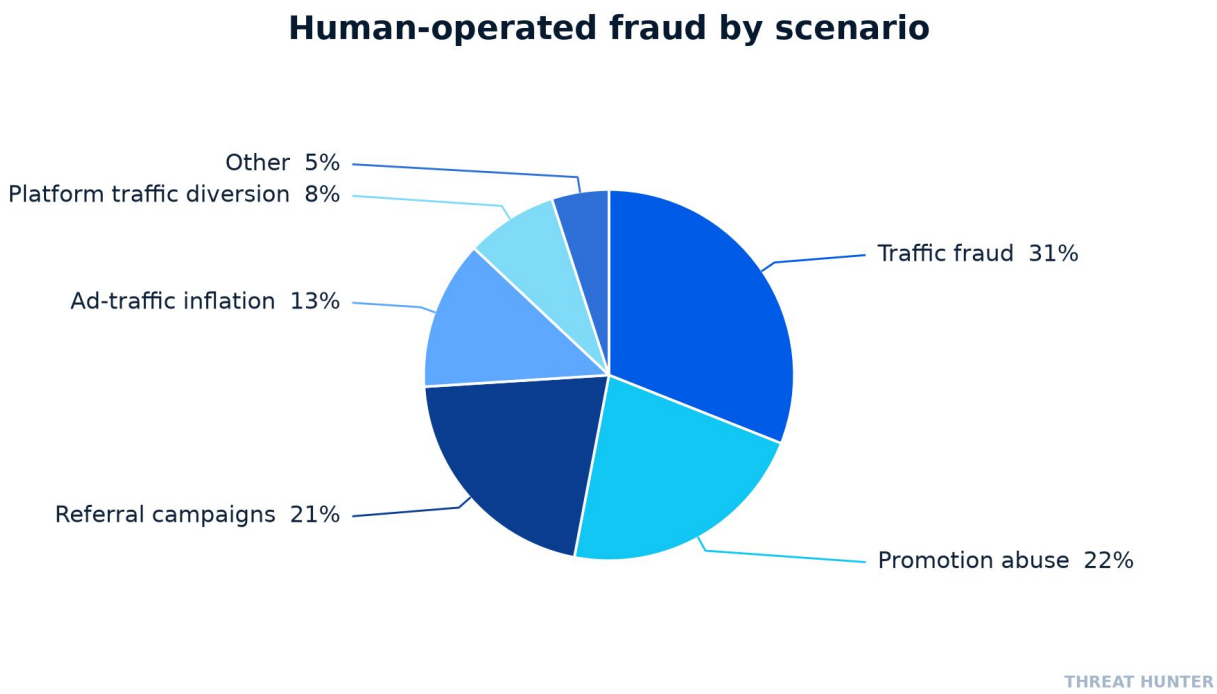
Target industries of human-operated fraud: banking and finance lead with 26%

Source: Threat Hunter original report, page 6. Redrawn in English from the original figure.

Figure 2-1 Proportion of human-operated fraud target industry types

2.1.2 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:



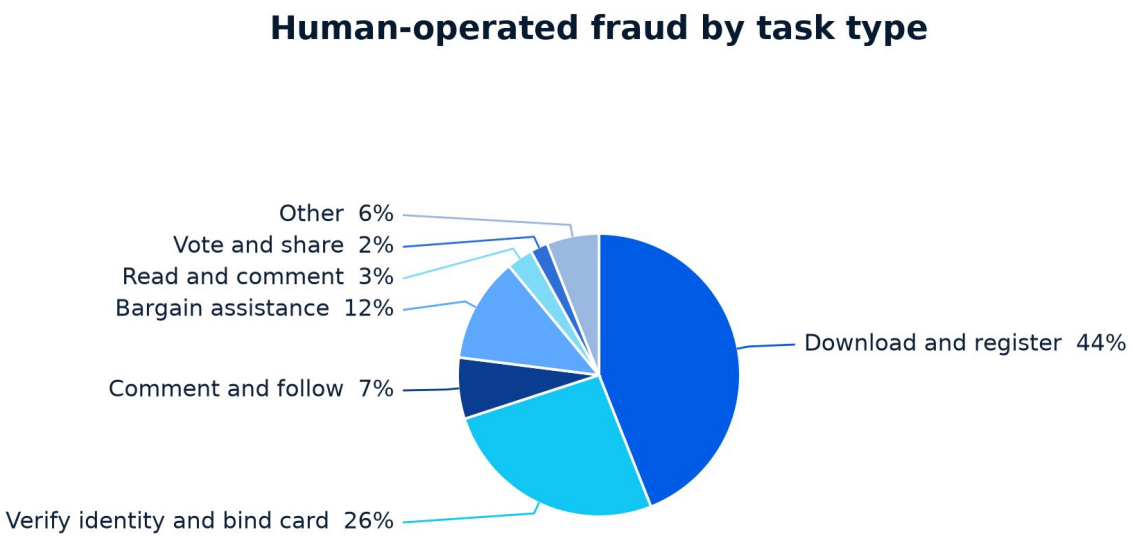
Scenarios targeted by human-operated fraud: traffic fraud is the largest at 31%

Source: Threat Hunter original report, page 7. Redrawn in English from the original figure.

Figure 2-2 Proportion of human-operated fraud scenario types

2.1.3 Multi-task 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 8. Redrawn in English from the original figure.

Figure 2-3 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. From this, 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 9. Redrawn in English from the original figure.

Figure 2-4 Word cloud diagram of human-operated fraud task types

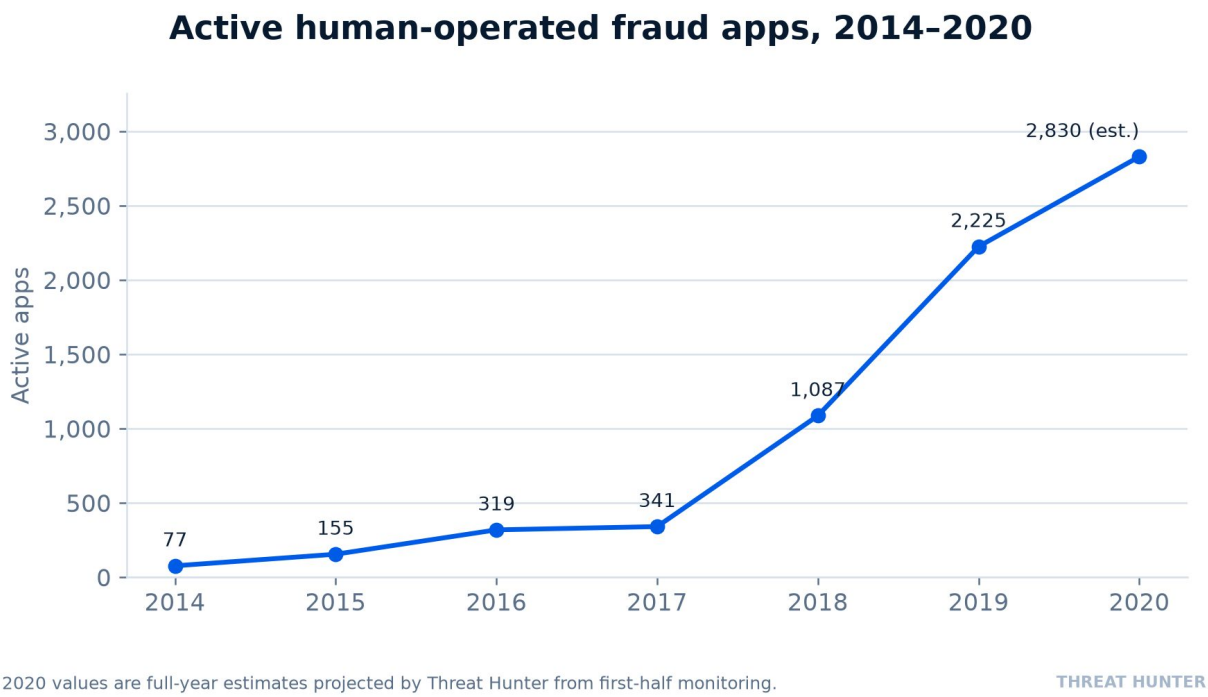
2.2 Human-operated fraud apps have expanded rapidly

2.2.1 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, instant-messaging groups used by the cybercrime ecosystem, 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.

Long: In 2014, there were less than 100 models, but this year, there are nearly 3,000 models, as shown in the figure below:

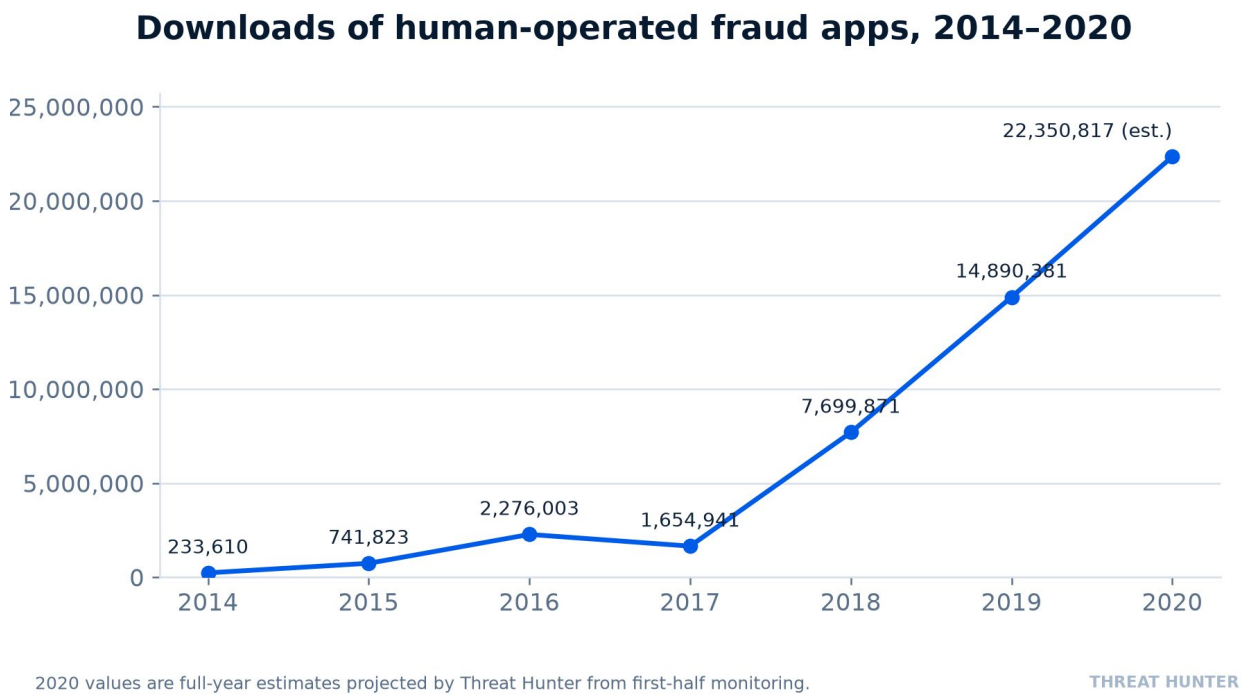


Active human-operated fraud apps, 2014 to 2020: from 77 to an estimated 2,830

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

Figure 2-5 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

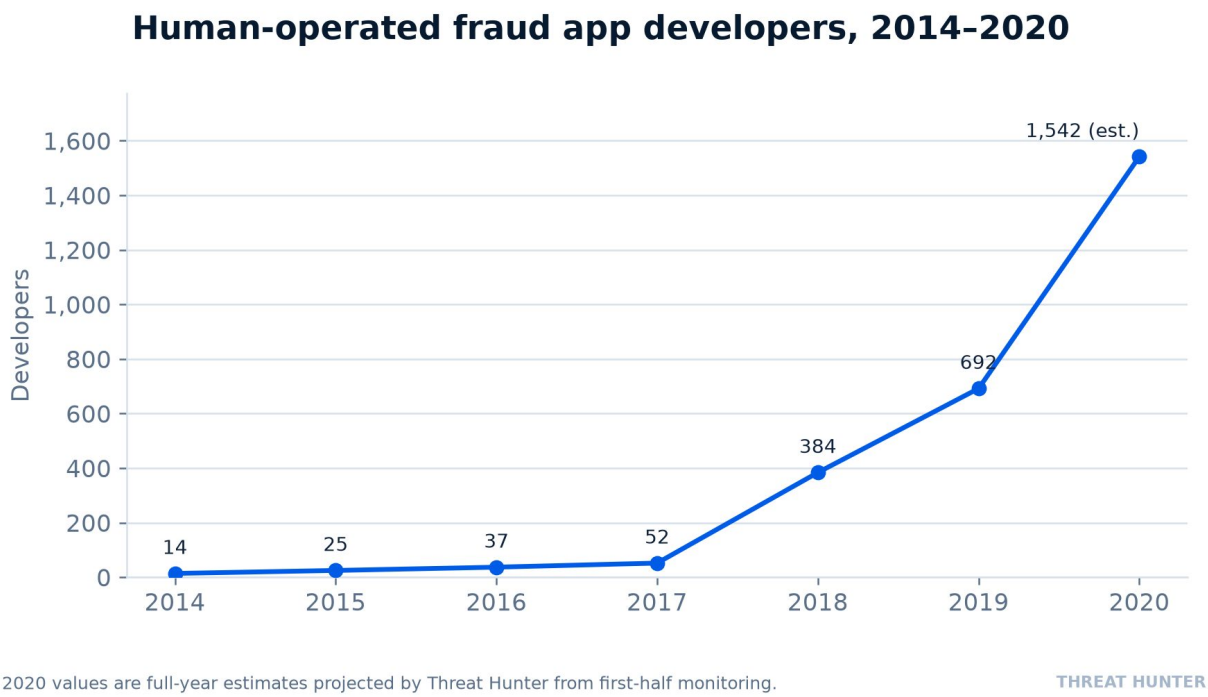
Source: Threat Hunter original report, page 10. Redrawn in English from the original figure.

Figure 2-6 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 and the development status of human-operated fraud, we reasonably speculate that: in the second half of 2020

The number of downloads of the human-operated fraud app can be increased by another 10,000,000 times, and the final number of downloads for the whole year is: 22,350,817 times.)

2.2.2 Developers grow rapidly from 2014 to 2020

Behind the explosive growth in the number of participants in human-operated fraud, it 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. From the data monitored by Threat Hunter, we can find that the number of developers of human-operated fraud apps has also shown exponential growth: from less than 20 in 2014 to about 1,500 this year, the development rate is astonishing.

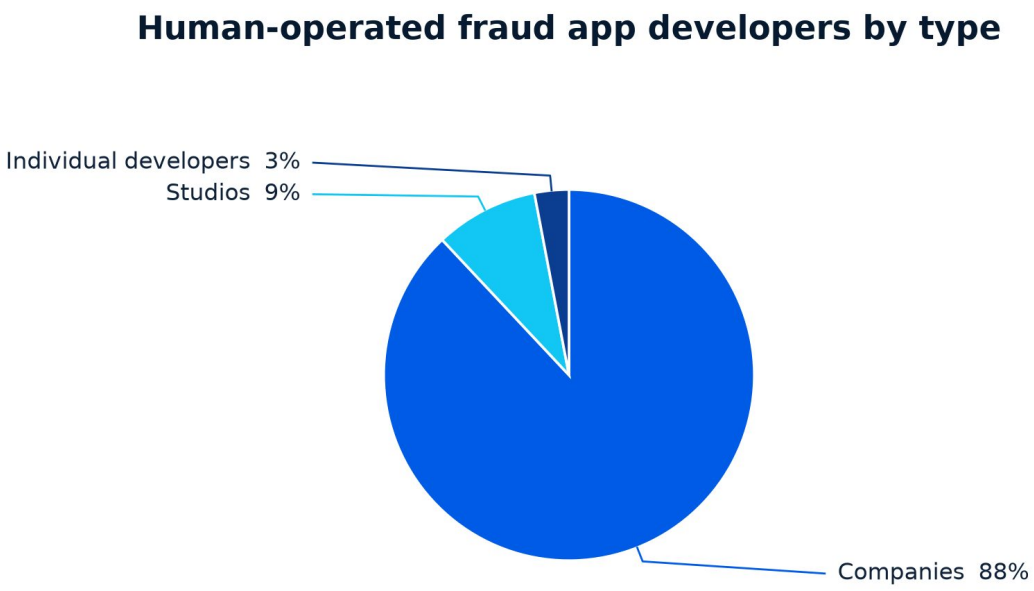


Human-operated fraud app developers, 2014 to 2020: from 14 to an estimated 1,542

Source: Threat Hunter original report, page 11. Redrawn in English from the original figure.

Figure 2-7 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 current 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.

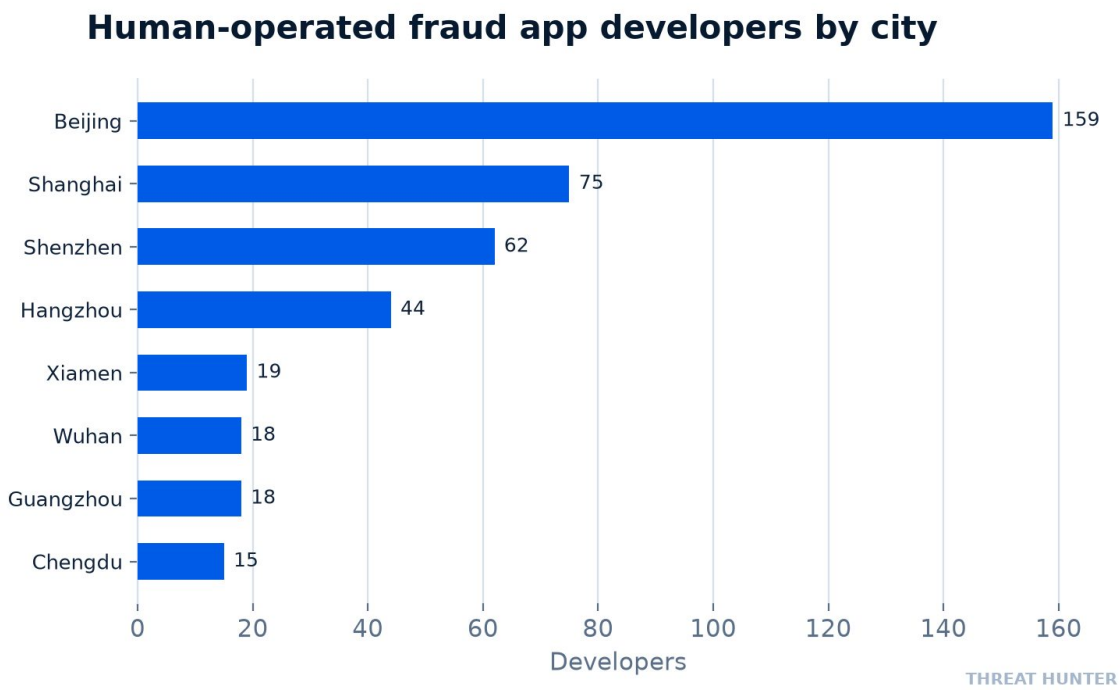


Developers of human-operated fraud apps by type: 88% are companies

Source: Threat Hunter original report, page 12. Redrawn in English from the original figure.

Figure 2-8 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 12. Redrawn in English from the original figure.

Figure 2-9 City distribution of real-life cheat developers

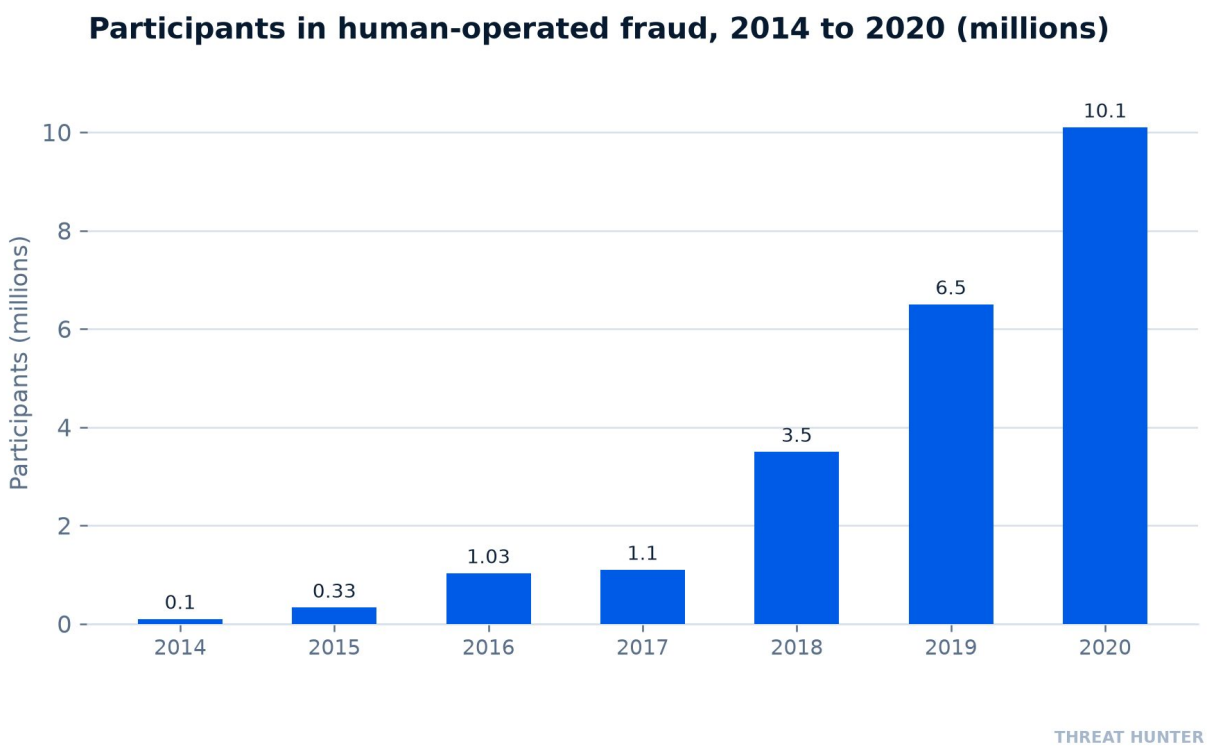
What's more, some companies have developed many human-operated fraud apps at the same time. For example, a company in Bengbu has developed 23 human-operated fraud apps at the same time; a company in Qingdao has developed 10 human-operated fraud apps at the same time, etc. As the saying goes, if there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

2.3 Profile of participants in human-operated fraud

So, what are the characteristics of users who participate in human-operated fraud? Please see the following portrait description.

2.3.1 Number of people in the human-operated fraud industry

The rise of any industry is inseparable from human participation. As seen above, whether it is the diversity of human-operated fraud tasks or the booming development of apps, it is 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:



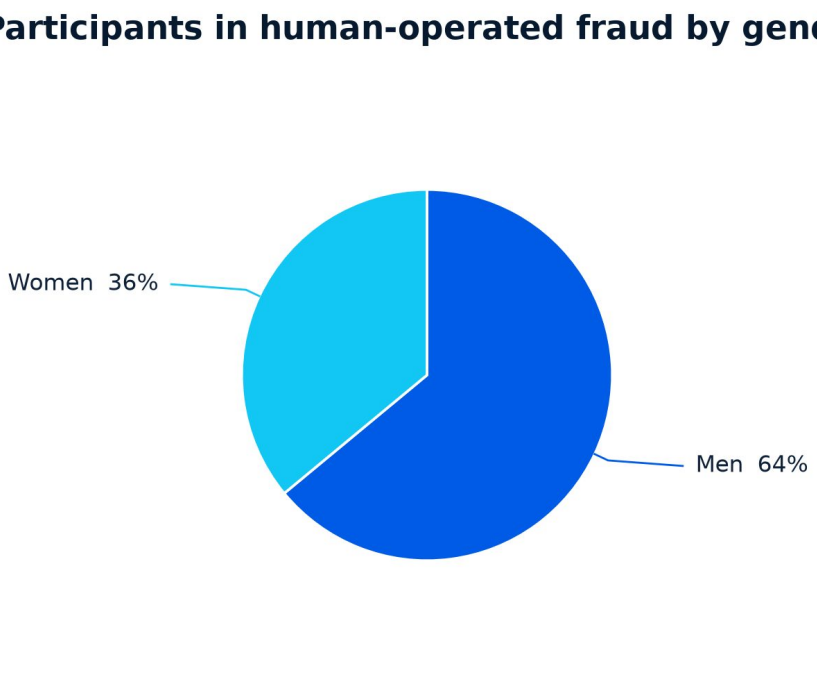
Participants in human-operated fraud grew from about 100,000 in 2014 to 10.1 million in 2020

Source: Threat Hunter original report, page 13. Redrawn in English from the original figure.

Figure 2-10 The development trend of the number of participants in human-operated fraud

2.3.2 Male to female ratio of real cheaters

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:



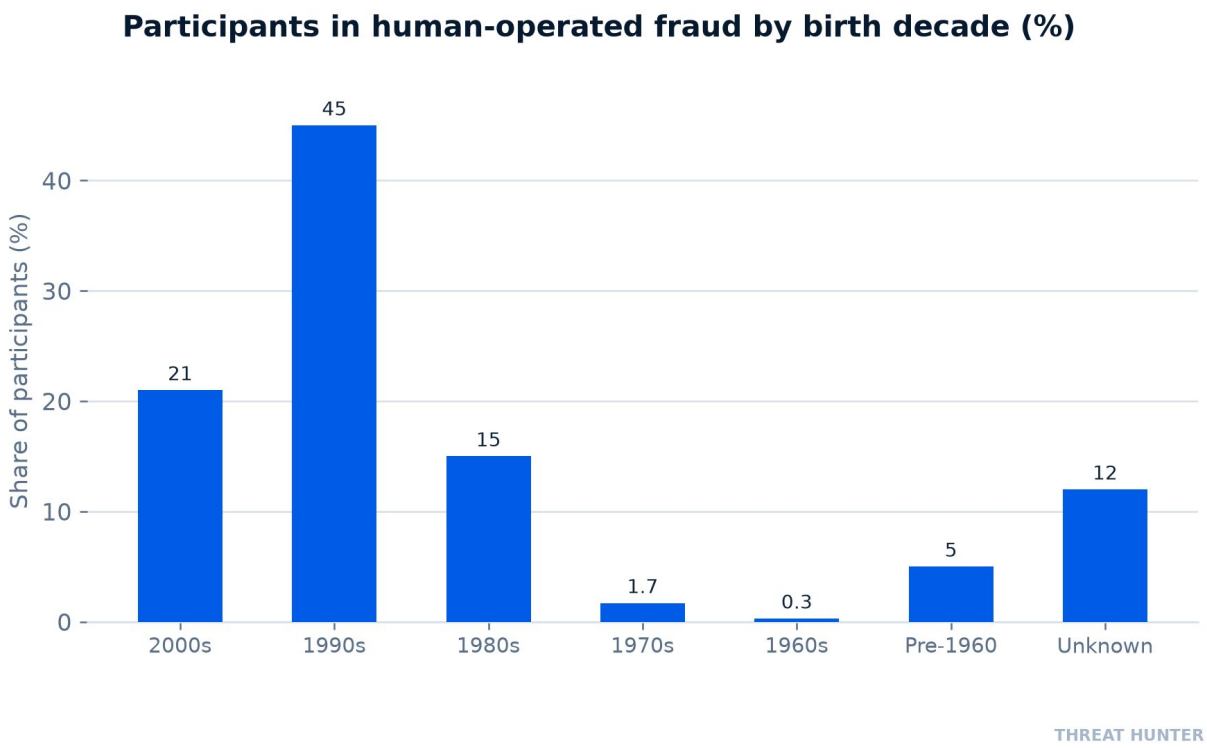
Participants in human-operated fraud by gender: 64% men, 36% women

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

Figure 2-11 Male to female ratio of human-operated fraud participants

2.3.3 Age distribution of real cheaters

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 that the human-operated fraud industry will continue to develop.



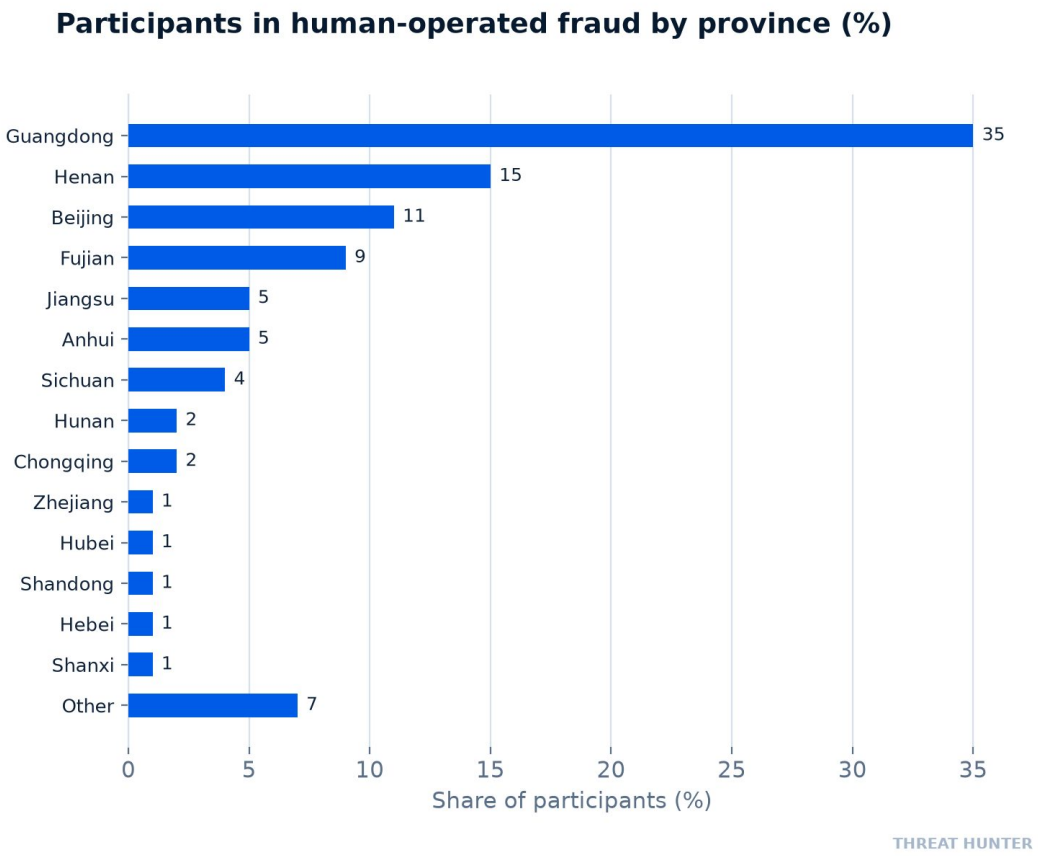
Participants by age group: people born in the 1990s are the main force at 45%

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

Figure 2-12 Age distribution of human-operated fraud participants

2.3.4 Geographic distribution of participants in human-operated fraud

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 15. Redrawn in English from the original figure.

Figure 2-13 Geographical distribution of human-operated fraud participants

2.4 Industry losses associated with human-operated fraud

So how much damage does human-operated fraud cause to various industries?

Threat Hunter has conducted comprehensive statistics on the human-operated fraud platform tasks in the past six months, with the number of bounties, bounties

The amount, number of completions, bounty time, completion time and other factors were calculated, and the following conclusions were drawn:

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

3. Pain points and hazards

3.1 human-operated fraud vs automated fraud table 3-1 Comparison of the characteristics of human-operated fraud and 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 17. Table re-typeset in English from the original.

3.2 human-operated fraud vs traditional fraud controls Traditional fraud controls is based on the resources of threat actors and the characteristics of “abnormal people” exhibited by threat-actor groups.

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", 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 at the rule level, or the AI algorithm, decision 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, human-operated fraud crowd behavior, portraits, user relationships and other characteristics are often discrete and varied. Although it is not completely traceable, the input of the algorithm model strongly relies on the security personnel's insight and analysis ability 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 be compatible with fraud-control indicators and user experience, how to provide highly explainable handling reasons to the business team, etc. These are further tests for the fraud-risk team.

step upgrade.

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 retrieval. Real users are between threat actors and victimized 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.

3.3 Additional risks created by human-operated fraud

In addition to fake orders, fake transactions, 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, judging from the income-to-output ratio, threat actors are willing to pay such a high commission, indicating that threat actors' income is likely to reach a hundred yuan or more, so for the financial platform that promotes it, it will inevitably suffer a lot of losses; secondly, when we were chatting 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:



A task publisher asks a participant for name, phone, ID and bank card details

Source: Threat Hunter original report, page 19. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	I am ...
2	How does it work?
3	Send me your details
4	Submit details (as follows)
5	1. Name + phone number + ID number + bank card
6	2. Phone number registered with the bank card

Figure 3 - Chat 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. Names, phone numbers, ID cards, bank cards and SMS verification codes are very sensitive personal information and are completely exposed to the control of threat actors. Personal information and even property security are seriously threatened.

4. Confrontation and Resolution

Such surging human-operated fraud has various advantages over machines, and it also poses a direct challenge to traditional fraud controls, making the challenges increasingly 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 participants fraud.

4.1 Intelligence Dimension

For example, when Threat Hunter conducted comprehensive monitoring of human-operated fraud platforms last year, it discovered some tasks with information similar to this:

"Register and download XX software, set the password to a123456, and contact me for payment after completion." After that, we followed the clues and found nearly 100,000 similar related tasks among the remaining hundreds of human-operated fraud platforms, and their password setting requirements were the same. This clearly 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 carried out reverse tracing and positioning as soon as possible. As a result, a large-scale gray production gang was indeed uncovered and successfully cracked down. This directly maintained the safety and harmony of the platform and nipped the damage in the cradle.

4.2 Data Dimension

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 of human-operated fraud tasks, links, tutorials, task processes, etc.

For example, starting in May this year, a certain domestic payment platform began to attract new customers and bind 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, such activities require real names, bank cards, etc., and the cost and threshold of automated fraud are high, so cybercrime ecosystem with specific channel resources began to publish tasks on many human-operated fraud platforms (after long-term follow-up research, we found that some cybercriminal groups have a large amount of cash back resources, which they call "kouzi").

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.

5. Write at the end

When companies rack their brains and think hard to deal with cybercrime ecosystem, cybercriminal groups can always find the company's security shortcomings and seize profits; when companies think they have finally caught up with cybercriminal groups' footsteps and secretly think that they can defend cybercrime ecosystem from the door, in fact they only see the heels of cybercrime ecosystem; when companies implement 360-degree protection and adopt various advanced rule algorithm models, cybercriminal groups began to "return to the basics" and use the simplest human-operated fraud methods to fight against the most advanced technology. The road to fraud controls is long, and security must not be lax. In the face of the ever-evolving cybercrime ecosystem, pure technical attack and defense will be stretched thin. Only by following the pace of cybercrime ecosystem in a timely manner can we not be too passive.

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 deep 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 the iteration of the fraud-decision engine, and thereby improves the overall offensive and defensive efficiency of the enterprise.