THREAT HUNTER RESEARCH

Q3 2023 Cybercrime Ecosystem Research Report

A third-quarter review of attack resources, AI-enabled identity abuse and the convergence of cybercrime and data exposure.

Original publication: 2023-10-26
Research team: Threat Hunter Research Team
Source report: 36 pages

Original report text

This text version is reconstructed based on the 36-page original PDF, retaining the report narrative, chapters and research scope; the cover, duplicate table of contents and purely decorative pages are not repeated. Localized figures are placed in context throughout this web edition, with the original PDF retained for reference.

Preface

In recent years, the cybercrime ecosystem chain has continued to mature and grow. Its attack technologies and resources have been rapidly updated, and the confrontation between enterprises and threat actors has become increasingly fierce.

Questions such as "Which threat actors are attacked", "What technologies/resources will threat actors use to attack", and "What risks are faced" still trouble the internal security operations personnel of the enterprise.

Relying on the long-term monitoring and mining of threat actors intelligence and the research on threat actors attack and defense, Threat Hunter has comprehensively sorted out and analyzed the potential risks of enterprises from the dimensions of attack resources used by cybercriminal groups, business fraud scenarios, and data leakage scenarios in the third quarter of 2023. It hopes to help more enterprises gain a deeper understanding of the cybercrime ecosystem, effectively prevent and control various attack risks, and avoid losses.

Analysis of attack resources used by cybercriminal groups in the third quarter of 2023

1. Analysis of attack resources used by cybercriminal groups in the third quarter of 2023

1.1 Analysis of the new increase in illicit SIM cards in the third quarter

1.1.1 The total number of illegal mobile phone card captures in the third quarter decreased by 26.27% compared with the second quarter.

According to data from the Threat Hunter business risk intelligence platform, the total number of illegal mobile phone card captures in the third quarter of 2023 dropped by 26.27% compared with the second quarter.

According to analysis by Threat Hunter intelligence experts, the main reasons for the continued decline are:

In early August, a leading number-receiving platform was shut down, resulting in a large number of illicit SIM cards suppliers and threat actors using illicit SIM cards being unable to supply and use illicit SIM cards normally, thus affecting the circulation of black phone numbers. Affected by this, the "monthly new increase" of illicit SIM cards also continued to decline in the third quarter.

1.1.2 The number of new interception cards continued to decline in the third quarter

The number of new interception cards continued to decline in the third quarter of 2023. The number of new interception cards in the third quarter was only 47% of that in the second quarter.

According to analysis by Threat Hunter intelligence experts, the main reason for the decline is that since April 2023, the number of new interception cards provided by the three head SMS verification-code receiving services has continued to decrease, which has led to a continued decrease in the number of new interception cards.

1.1.3 The usage of Section 192 in the third quarter increased by 123% compared with the second quarter

According to data from the Threat Hunter business risk intelligence platform, in the third quarter of 2023, the usage of illicit SIM cards in Section 192 was 2.23 times that in the second quarter.

According to analysis by Threat Hunter intelligence experts, the main reason for the large increase in the third quarter is that since the first quarter, various black card supply channels have continued to invest in new No. 192 mobile phone cards. At the same time, since the third quarter, 4 supply channels have further increased the investment scale of mobile phone cards in segment 192, further increasing the new increment in the third quarter.

1.2 Analysis of risk IP capture volume in the third quarter

1.2.1 The total amount of risky IP captured in the third quarter increased by 2.8% compared with the second quarter

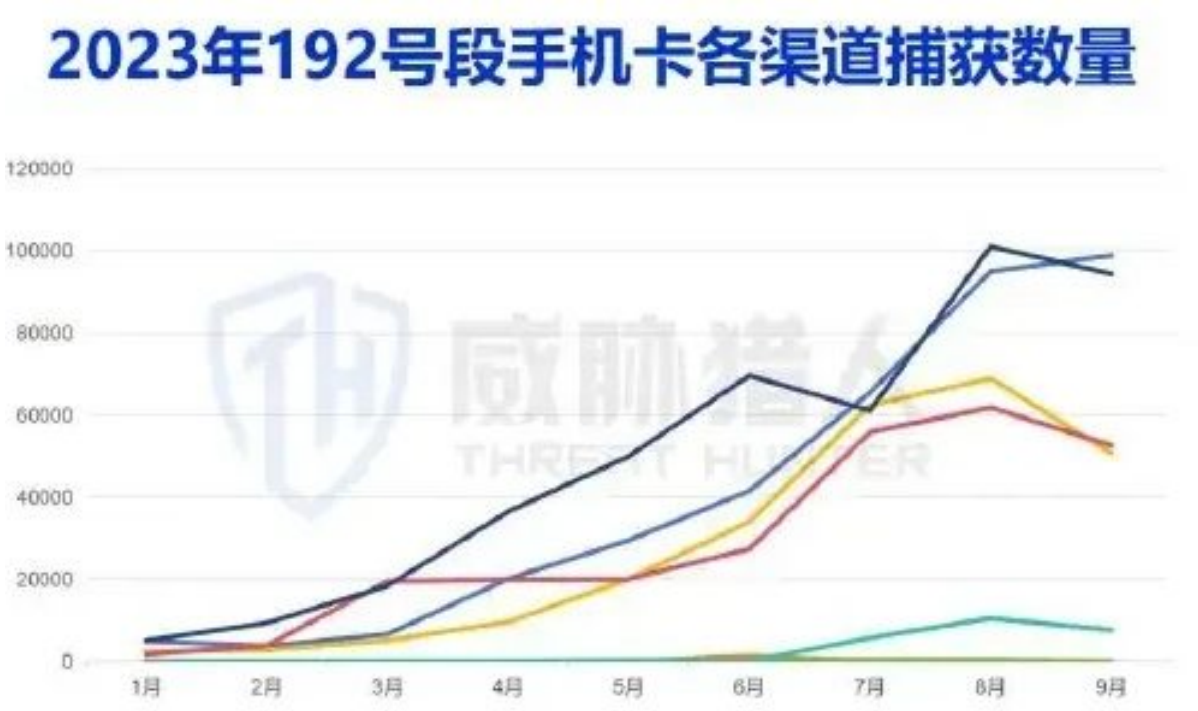
The total amount of risky IP captured in the third quarter of 2023 increased by 2.8% compared with the second quarter, and the data did not fluctuate significantly.

1.2.2 Trojan disguises itself as normal software and uploads normal user IP to the proxy platform

Threat Hunter researchers found that normal user IPs appeared in the IP pool of the proxy IP platform in the third quarter, showing a clear upward trend. This situation will cause the operation behavior of an IP to include both normal user behavior and threat actors' malicious behavior in a short period of time.

The business performance of this type of IP is as follows: Most of the time, normal users perform operations, such as clicking, recharging, browsing, etc., but short-term malicious behaviors may occur in a small amount of time. Therefore, for customer fraud controls, the platform will identify the user as a normal user and then ignore his short-term malicious behavior, giving threat actors an opportunity to take advantage.

At the same time, Threat Hunter researchers traced the source of the malicious tools behind it, which disguise Trojans as normal software for users to download and use. After the user installs and runs the tool for the first time, the Trojan can upload the IP of normal users to the proxy platform for threat actors to use for malicious purposes.



The third quarter, 192, up from the second quarter, 123%.

Source: Threat Hunter original report, page 7

English figure labels

1	Numbers captured by mobile card channels in sector 192, 2023

Taking the captured "xx accelerator" tool as an example, its malicious process is:

(1) After a normal user installs "xx Accelerator" on the computer, the program releases the Trojan file to the specified location;

(2) Trojans inject specific processes and hijack user IPs to perform arbitrary operations;

(3) The Trojan maintains its operating authority through a specific method to achieve the purpose of "the Trojan can still run after the accelerator is turned off";

(4) Run the real accelerator program for users to use.

The researchers extracted three executable programs through technical analysis, which were recorded as samples A, B, and C:

Sample A: An executable program sample that implements the Trojan loading function B: An executable program sample that maintains Trojan resident permissions C: A real accelerator client

Sample A:

Through analysis, it can be determined from the functional perspective that sample A is a Trojan loader, which has the function of decrypting binary code and loading PE into memory.

Sample B:

Through analysis, it can be determined from a functional perspective that the main function of sample B is to create services and maintain Trojan residency permissions.

1.3 Analysis of Risk Email Capture Volume in the Third Quarter

1.3.1 The total number of risk mailbox captures in the third quarter increased by 71.16% compared with the second quarter

In the third quarter of 2023, Threat Hunter continued to cover and monitor temporary mailbox websites, and statistics found that the total number of risky mailboxes captured in the third quarter increased by 71.16% compared with the second quarter.

1.3.2 Temporary mailboxes used by threat actors to conduct malicious activity show obvious gang aggregation characteristics

Overseas, email registration is still one of the main methods of account registration. Due to its low cost, anonymity, and one-time use, temporary mailboxes have become the preferred material for threat actors to attack overseas businesses.

Threat Hunter researchers analyzed the MX, IP and domain name registration information of the 46,737 captured valid temporary email domain name samples, and found that 66.65% (a total of 31,150) email domain names have common characteristics and can be associated with multiple criminal gangs.

After classifying the above 31,150 email domain names, six groups of threat actors can be sorted out, and multiple temporary mailboxes under the same group often show characteristics of aggregation. Some gangs have "strong association" features, and as long as they appear, they can be determined to be from the same gang; some gangs have "weak association" features, which require a combination of multiple features to determine:

Take the group with the most temporary mailboxes as an example: 10,085 mailbox domain names resolve to the same MX (mail.***.kr), and the mailbox suffix is basically xxx.kr, which can be directly determined to be from the same group. The characteristics of the email addresses associated with this group are as follows:

1.4 Analysis of online money laundering resources in the third quarter

通过分析，从功能上可以判定样本 A 是一个木马加载器，它具备解密二进制代码、内存加载 PE 的功能。

功能	解释
功能一	解密二进制数据，然后通过内存加载的方式，将解密后的PE代码加载到进程空间
	手动转存解密后的二进制数据，发现是一个DLL，该DLL是Farfli木马家

Ponys disguised as normal software upload normal user IP to proxy platform (Chart 1)

Source: Threat Hunter original report, page 10

English figure labels

1	The function of carrying PE.
2	Function I

样本 B:

通过分析，从功能上可以判定样本 B 的主要功能是创建服务，维持木马驻留权限。

功能	解释
功能一	解密出C2地址：hackerXXXXXX.XXXXXX.net:8088，在受害者机器上线前使用互斥体来判断是否存在多个运行实例，防止重复上线。
	维持木马驻留权限。

Ponys disguised as normal software upload normal user IP to proxy platform (Chart 2)

Source: Threat Hunter original report, page 10

English figure labels

1	Sample B:
2	From the analysis, it is functionally possible to determine that the main function of sample B is to create services and maintain the presence of wooden horses.
3	Decrypt C2 address: hackerXXX.XXX.net8088 in victim machine Let's go.
4	Function I
5	The front-line use of retrusion to determine whether there are many operational examples to prevent re-entry.
6	Even if it's true.

1.4.1 Among the various channels of online money laundering resources in the third quarter, third-party payment platforms accounted for

Reported share: 72.63%

Among the money laundering resource channels in the third quarter of 2023, the largest proportion is third-party payment platform accounts, followed by virtual currency trading platform accounts, bank cards, and digital RMB accounts.

1.4.2 The amount of digital RMB captured in the third quarter increased significantly in September, with a monthly increase of over 270%

Threat Hunter found that the use of digital renminbi for money laundering by threat actors is on the rise overall, especially in September, with a monthly increase of more than 270%.

According to analysis by Threat Hunter intelligence experts, the main reason for the large increase is that a large number of new four-party payment platforms that support digital renminbi money laundering appeared in September, an increase of 39 platforms compared with August.

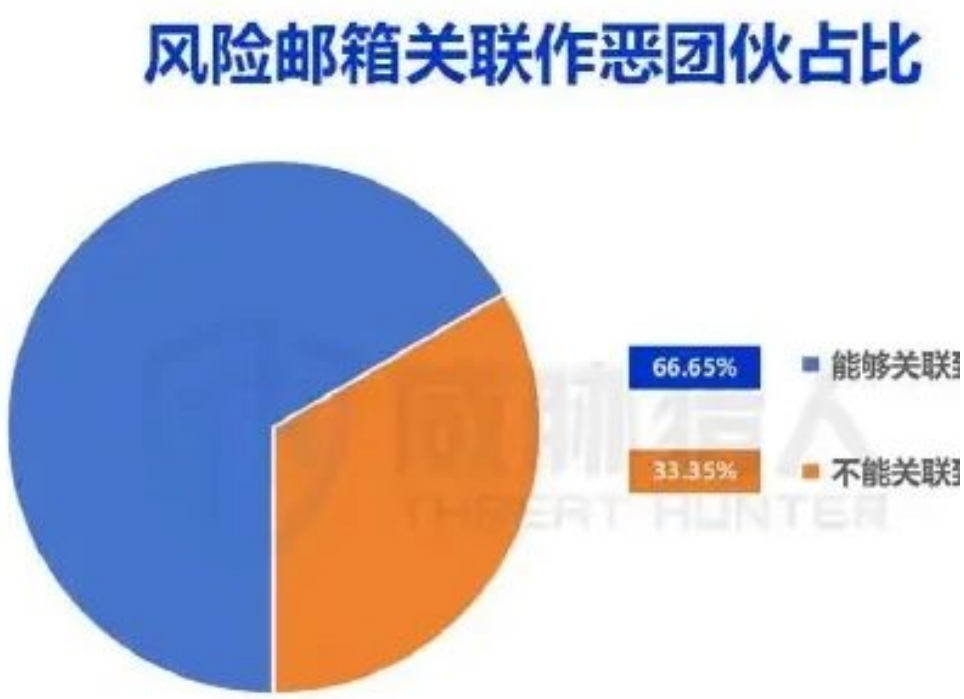
In addition, although the number of four-party payment platforms in the second quarter was similar to that in the first quarter, Threat Hunter intelligence experts found that since May, some four-party payment platforms have begun to increase the frequency of money laundering through the digital renminbi channel, causing the number of digital renminbi money laundering record captures to begin to increase.

1.4.3 In the third quarter, the total number of public accounts captured involving money laundering increased compared with the second quarter.

Reported share: 37.86%

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

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



Temporary mailboxes that have been used for abuse in cybercrime, showing a clear concentration of groups (Chart 1)

Source: Threat Hunter original report, page 12

English figure labels

1	Percentage of risk mailboxes associated with gangs
2	= Unconnected

同一团伙；有的团伙是“弱关联”特征，需要多个特征结合来判定：

Temporary mailboxes used for abuse in cybercrime, showing a clear concentration of groups (figure 2)

Source: Threat Hunter original report, page 12

English figure labels

1	“The characteristics of a gang within the same mission” require a combination of characteristics to determine:
2	Mailbox domain parsing MX
3	Same registration and short interval between registrations
4	*MX resolves IP1 to
5	Domain name server 1 to
6	Registration information I

Since March 2023, Threat Hunter has continued to cover and monitor bank account resources used by threat actors in the money laundering process, and found that the number of public accounts involved in money laundering continues to increase.

Analysis of business fraud scenarios in the third quarter of 2023

2. Analysis of business fraud scenarios in the third quarter of 2023

2.1 cybercriminal groups are connected to the AI robot, making social traffic flow more intelligent

Threat Hunter intelligence researchers discovered in the third quarter that cybercriminal groups have been connected to AI robots in social traffic scenarios, making traffic chats more intelligent. Take the captured automatic chat tool "AiTuLing" as an example. In addition to the conventional "draining traffic based on preset words", this tool also supports access to AI robots. At the same time, this tool supports automatic traffic drainage from nearly a hundred social platforms on the market.

团伙	强关联特征：邮箱域名解析到的mx	弱关联特征：邮箱域名的二级域名	弱关联特征：登记人	弱关联特征：注册邮箱	弱关联特征：域名服务器
		二级域名有66个，格式均为xxx.kr	Y**N	ax*****d@gmail.com	***.tad.cc、***.tad.cc
		nice***.com			N***.HO***NG.CO.KR
		ho*****.com		***@naver.	N***.HO***NG.CO.KR

Channels of Internet money-laundering resources in the third quarter (Chart 1)

Source: Threat Hunter original report, page 13

English figure labels

1	Parsed mx
2	There are 66 secondary domain names.
3	Format all xx.kr

Channels for Internet money-laundering resources in the third quarter (Chart 2)

Source: Threat Hunter original report, page 13

English figure labels

1	Third parties
2	m virtual
3	Digital

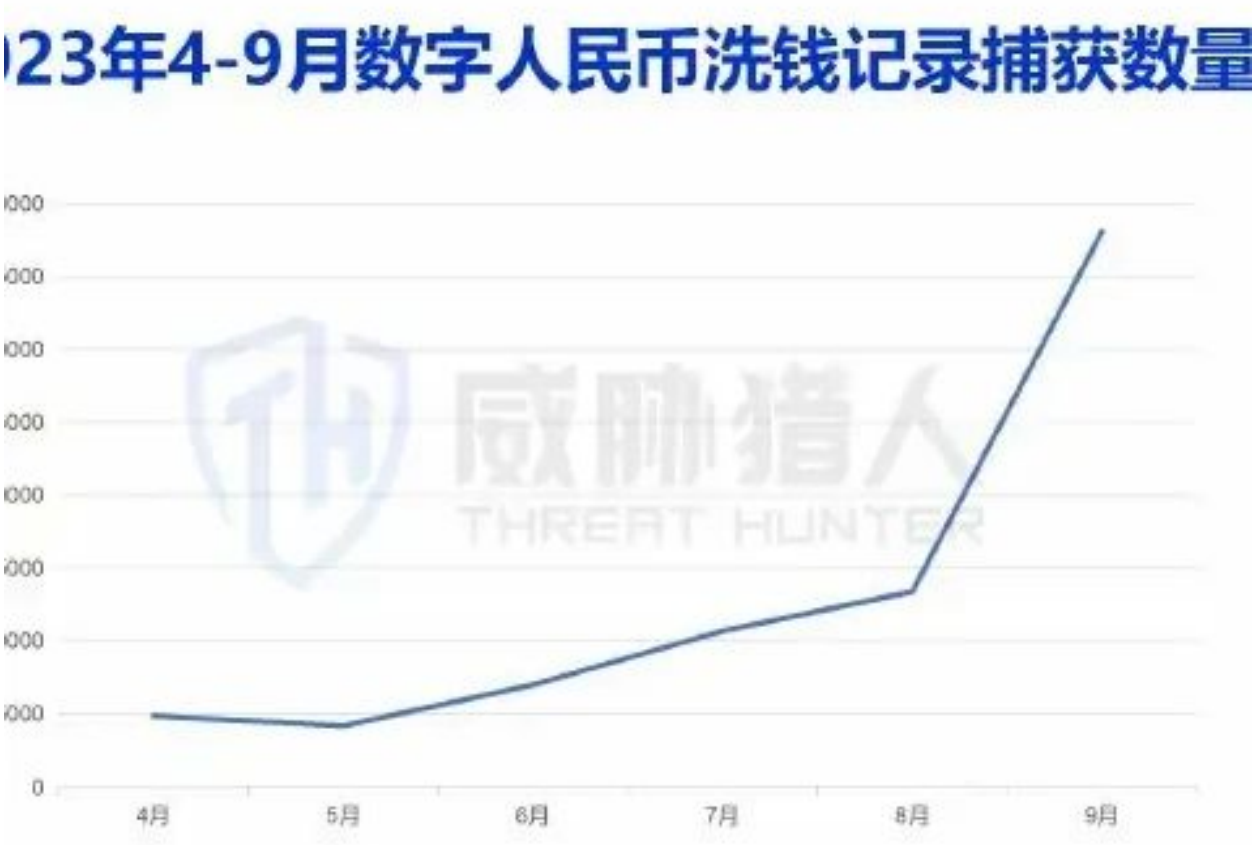
Compared with traditional preset words for reply and traffic, the characteristics of the two are as follows:

In terms of usage costs, the access cost of AI robots is also extremely low, with a minimum of only 19.9 yuan/month. Currently, such traffic diversion tools are mostly used by cybercrime ecosystem in social scenarios to divert traffic for downloads and preliminary screening of pornographic fraud targets, posing new challenges to the content fraud controls of social platforms.

2.2 The development of AI has reduced the cost of face replacement, and we need to be vigilant about the security of face verification.

In response to the recent hot cases of fraud based on AI face-changing technology, Threat Hunter researchers studied the relevant malicious tools and malicious processes, and finally successfully bypassed a bank's face authentication.

Research has found that the tools used by the cybercrime ecosystem when conducting malicious activity are as follows:



In the third quarter, there was a marked increase in the catch of the digital renminbi in September, which was more than 270 per month.

Source: Threat Hunter original report, page 14

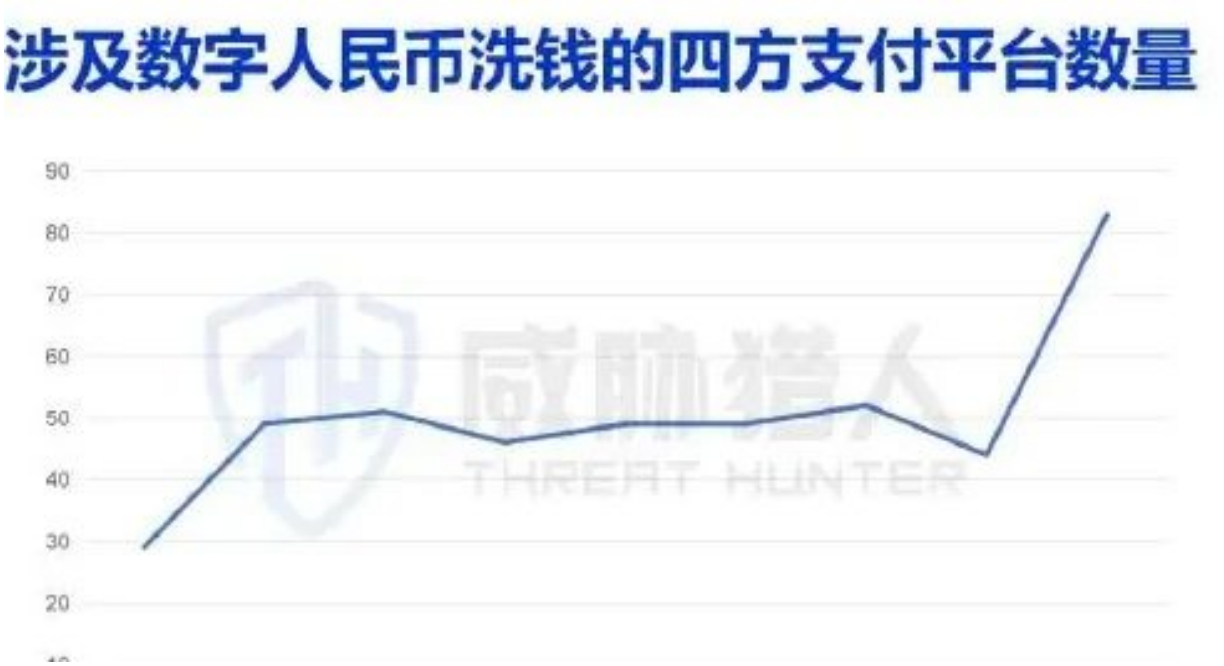
English figure labels

1	Number of seizures of digital renminbi money-laundering records, April-September 23, 2003

Threat Hunter researcher’s attack reproduction process is as follows:

(1) When logging in for the first time, the tester used his or her face to simulate the attacker's login to the victim's bank account, but failed to pass face authentication.

(2) For the second login, the tester used the victim's AI face-swapping video, and used a specific method to make the "face-swapping video picture" as the picture obtained by the login device camera, logged in to the victim's bank account again, and finally passed face authentication and successfully logged in.



Total catches of public accounts involving money-laundering increased in the third quarter compared to the second quarter

Source: Threat Hunter original report, page 15

English figure labels

1	Number of quadripartite payment platforms involving money-laundering of digital renminbi

2.3 cybercrime ecosystem account registration and bypass detection methods are becoming more diverse

Accounts are the basis for cybercriminal groups' attacks on the platform. However, due to different login methods between apps and the varying degrees of fraud controls in apps, different "account usage methods" will cause the account's service life on the platform to vary. In order to delay the use of malicious accounts to the maximum extent, threat actors introduce different methods of account registration and bypass detection for different situations.

The following is how some threat actors use malicious activity accounts organized by Threat Hunter:

Taking the backup package number to log in to social app as an example, the usage process is as follows:

2.4 cybercrime ecosystem combines lending platforms and virtual currencies to transfer money laundering risks

In the second quarter of 2023, Threat Hunter researchers discovered that some threat actors began to use lending platforms for money laundering, involving 27 lending platforms. In the third quarter, they found that the number of affected platforms increased to 41, an increase of 51.85% from the second quarter.

threat actors combine the loan platform with virtual currency, and with the help of a third party, use the money loaned out by the loan platform to purchase virtual currency that is difficult to regulate, and then use the black money as loan repayment funds and transfer it to the loan platform, transferring the risk of money laundering to the loan platform.

In past money laundering methods, threat actors directly used black money to purchase large amounts of virtual currencies on virtual currency trading platforms. This made the virtual currency accounts of threat actors easy for platforms to detect and restrict by the trading platform.

cybercrime access, AI, robotics, social influencing.

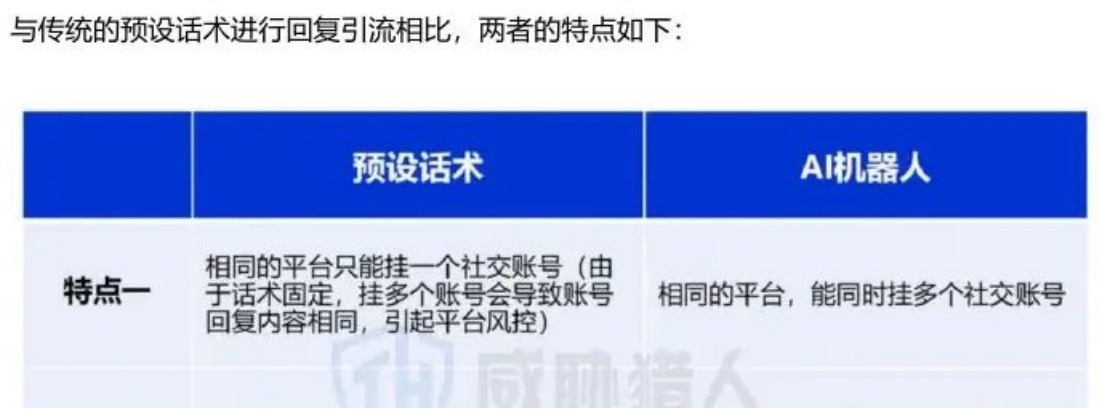
Source: Threat Hunter original report, page 18

English figure labels

1	Auto-direction.
2	Advertising notices
3	Name Switch
4	Sex One.
5	Tools run

Based on the method of "combining the loan platform with virtual currency", threat actors can transfer the operation of purchasing virtual currency to a third party. At the same time, because the third party's source of funds for purchasing virtual currency is normal, it can greatly reduce the possibility of detection by the virtual currency trading platform.

Regarding this type of money laundering method, Threat Hunter researcher summarized the process as follows:



cybercrime access, AI, robotics, social influencing.

Source: Threat Hunter original report, page 19

English figure labels

1	The features of both are as follows, compared to the traditional pre-characteristic response flow.
2	Characteristic I
3	It's fixed, it's the same platform, with multiple social accounts.
4	The same platform only has one social bill.
5	The response is the same, causing the platform to wind)

The final result of this money laundering method is:

2.5 cybercriminal groups use the iOS cloud devices provided by the cloud mobile phone platform to reduce the cost of iOS group control

Threat Hunter researchers discovered that some threat actors use iOS cloud mobile phones to conduct malicious activity. In response to this situation, the researchers conducted relevant research on the cloud mobile phone platforms currently on the market that provide iOS cloud mobile phone services. The survey results are as follows:

The risks brought by iOS cloud mobile phones for malicious purposes are as follows:

(1) The cost for threat actors to obtain iOS devices to attack and conduct malicious activity is reduced. In the past, attacks often required purchasing a real iPhone ranging from hundreds to thousands of yuan, but now it only costs tens of yuan/month to rent an iOS cloud phone.

(2) It saves the time required for threat actors to install and configure the malicious activity environment, and improves the attack efficiency of threat actors. The purchased iOS cloud phone

has been jailbroken and can install different jailbreak plug-ins. It also comes with modification tools, saving threat actors time in installing and configuring the malicious activity environment.

研究发现，黑灰产在作恶时使用的工具如下：

作恶工具类型	工具作用
AI换脸软件	基于目标人物的多角度图片或视频，进行换脸训练，并输出训

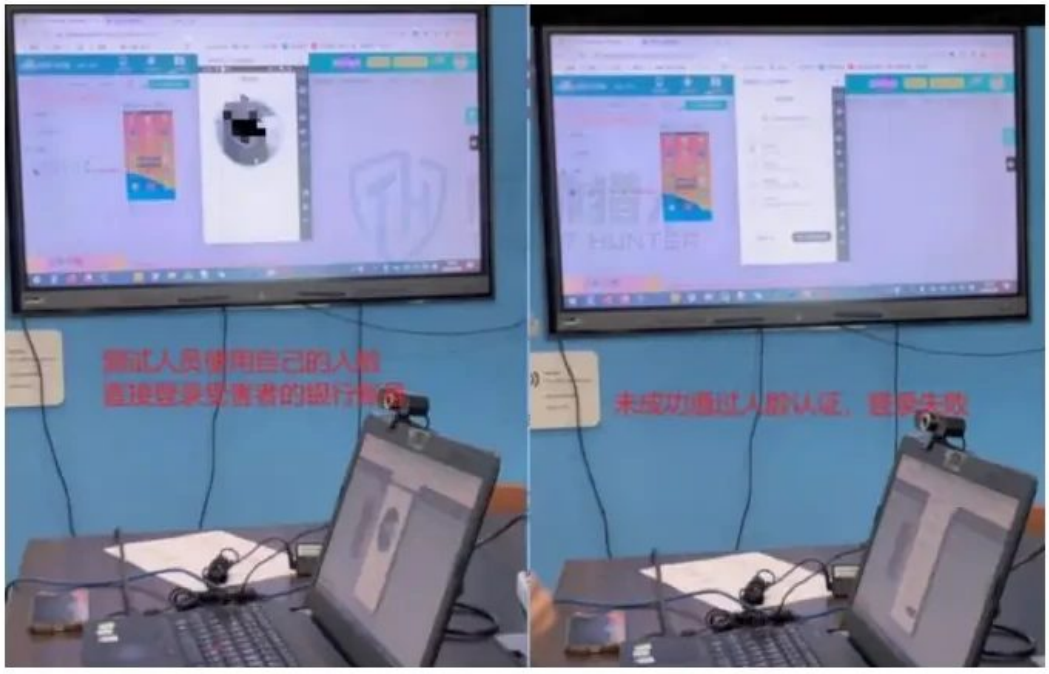
AI Development reduces the cost of face-to-face change and requires vigilance to verify safety (Chart 1)

Source: Threat Hunter original report, page 20

English figure labels

1	The study found that cybercriminal activity used the following tools in the commission of offences:
2	Training in face change based on multiple angles or videos of the target person, and output training

（1）首次登录，测试人员使用自己的人脸模拟攻击者登录受害者银行账号，未成功通过人脸认证。



AI Development reduces the cost of face-to-face change and requires vigilance to verify safety (Chart 2)

Source: Threat Hunter original report, page 20

English figure labels

1	(1) Initial log-in by tester using his face to simulate the victim ' s bank account, unsuccessfully passed

In addition, due to the strict restrictions on application permission application by the iOS system, it is much more difficult for most Internet companies to obtain device information on iOS devices than on Android devices. This may make it more difficult for the platform to conduct fraud-risk detection on iOS devices to a certain extent. Specifically, under the same attack process, threat actors using iOS devices to carry out attacks are less likely to be discovered by the platform, leading the cybercrime ecosystem to use iOS cloud phones as one of the main attack devices.

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

Analysis of data breach scenarios in the third quarter of 2023

3. Analysis of data leakage scenarios in the third quarter of 2023

的画面”作为登录设备摄像头获取到的画面，再次登录受害者的银行账号，最终通过人脸认证并成功登录。

Increased diversity of black-and-white account registrations and bypass tests

Source: Threat Hunter original report, page 21

English figure labels

1	Check and log in successfully.

3.1 Data breaches increased by 153% in the third quarter compared with the second quarter

In the third quarter of 2023, the Threat Hunter risk intelligence platform monitored more than 73 million pieces of data leakage-related intelligence and sorted out a total of 5,110 valid data leakage incidents, an increase of 153% from the second quarter.

3.2 In the third quarter, user information was still the main type of data leakage, accounting for 92.74%

The type of data breaches that occurred in the third quarter was still dominated by user information, accounting for 92.74%. In addition, there are also types of leaked information such as internal documents, internal employee information, and sensitive code.

3.3 Data breaches in the third quarter involved a wide range of industries, with the financial and logistics industries still being the hardest hit areas.

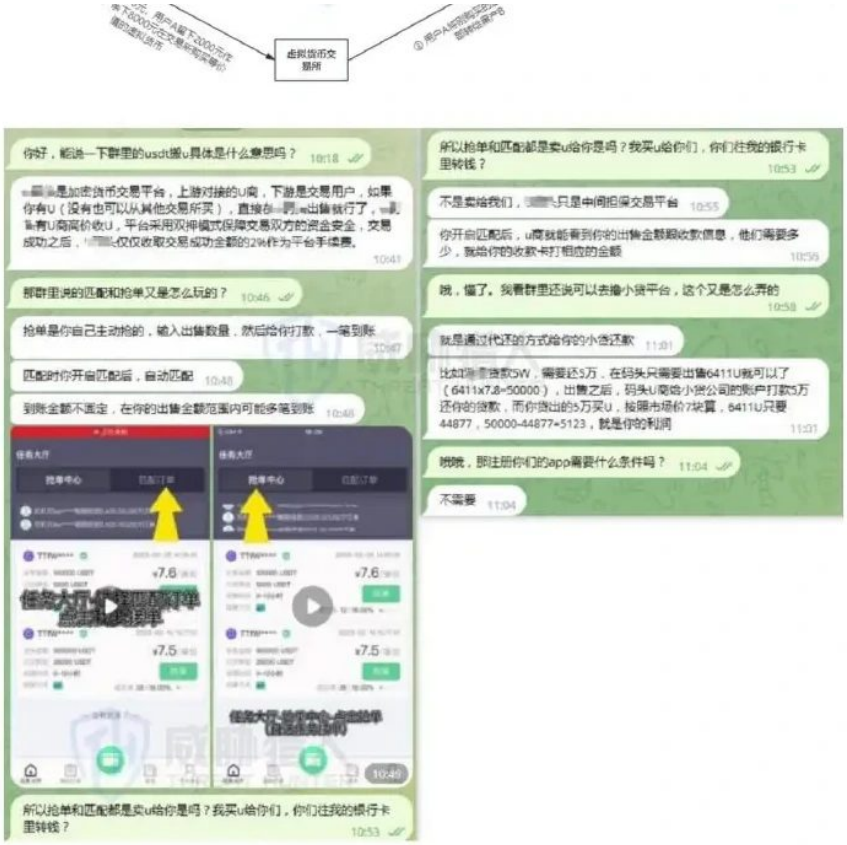
From the perspective of industry distribution, data breaches in the third quarter involved multiple industries, with the financial and logistics industries still being the hardest-hit areas.

3.4 The number of data breaches in the aviation industry continued to rise in the third quarter

The number of data breaches in the aviation industry increased by 253 compared with the second quarter, an increase of 337.33%.

According to analysis by Threat Hunter intelligence experts, the main reason for the continued increase is: affected by the recovery of the tourism market, domestic and international flights are booming, and attacks by threat actors around the aviation industry continue to increase, especially targeting the supply chains, agents and other links of major aviation companies. The final impact is that a large number of criminals use aviation data to commit fraud.

3.5 Analysis of typical data breach incidents in the third quarter



cybercrime ecosystem combined loan platforms and virtual currency to transfer money-laundering risks

Source: Threat Hunter original report, page 24

English figure labels

1	Upstream against U, downstream trade is a user.
2	You have U.
3	The deal.
4	When it's done, it's done. Continuation
5	What about this?
6	And you're paying $50,000 for U.
7	44877, 93 lire.
8	7 I'll buy you guys.

3.5.1 Case 1: Enterprise employee email information was leaked, resulting in employees being defrauded by phishing emails

In August 2023, Threat Hunter discovered on Telegram that employee email information of a domestic financial investment company was leaked, resulting in employees being subjected to email phishing scams by downstream threat actors.

According to analysis by Threat Hunter researchers, the main reason for this data leakage is that there is an API security vulnerability in the corporate mailbox, and threat actors used the vulnerability to brute force crack the corporate mailbox and steal employee mailbox information.

3.5.2 Case 2: A third-party platform illegally stored resumes on recruitment websites, involving more than 200,000 resumes

In August 2023, Threat Hunter security researchers discovered that resumes on a recruitment website were illegally stored by a third-party platform, involving more than 200,000 resumes, which contained a large amount of sensitive personal information of recruiters.

The third-party platform illegally stored the crawled resumes on its own rented server, and provided tools for its platform users to view the crawled resume information. Since the tool has built-in logic for accessing server data, including database addresses, account passwords, etc., and the tool can be publicly downloaded, professional hackers can analyze the tool, obtain database addresses, database account passwords and other information, and easily steal all resumes on the server.

Therefore, Threat Hunter recommends that enterprises use management software and tools developed by niche companies with caution. Due to the lack of security in data storage, sensitive data may be obtained.

Conclusion

4. Write at the end

cybercriminal groups are becoming increasingly rampant, causing serious harm to companies in various industries. Judging from the overall trend of cybercrime ecosystem big data in the third quarter of 2023, companies need to focus on the following risks:

1. The Trojan disguises itself as normal software and uploads the normal user IP to the proxy platform

The business performance of this type of IP is as follows: Most of the time, normal users perform operations, such as clicking, recharging, browsing, etc., but short-term malicious behaviors may occur in a small amount of time. Therefore, for customer fraud controls, the platform will identify the user as a normal user and then ignore his short-term malicious behavior, giving threat actors an opportunity to take advantage.

2. AI chat, AI face-changing and other technologies are used by threat actors, and the attack success rate is greatly increased.

1 For social platforms, the application of AI chat technology will make it more difficult to identify threat actors when conducting traffic diversion operations, while AI face-changing technology will significantly increase the success rate of threat actors using the video chat function to commit fraud.

2 For financial, payment and other platforms, most platforms currently use face authentication as one of the security verification measures for sensitive operations such as transfers. The popularity of AI face-changing technology will also cause the platform's face authentication to be bypassed, and user funds to be stolen frequently.

3. The number of data leakage incidents in the financial industry continues to rise, surpassing the logistics industry to become the most affected area.

The number of data leaks increased from about 1,000 in the first quarter to 5,110 in the third quarter.

Source: Threat Hunter original report, page 28

English figure labels

1	Number of captured data leaks in the first three quarters of 2023
2	First quarter
3	Second quarter
4	Third quarter

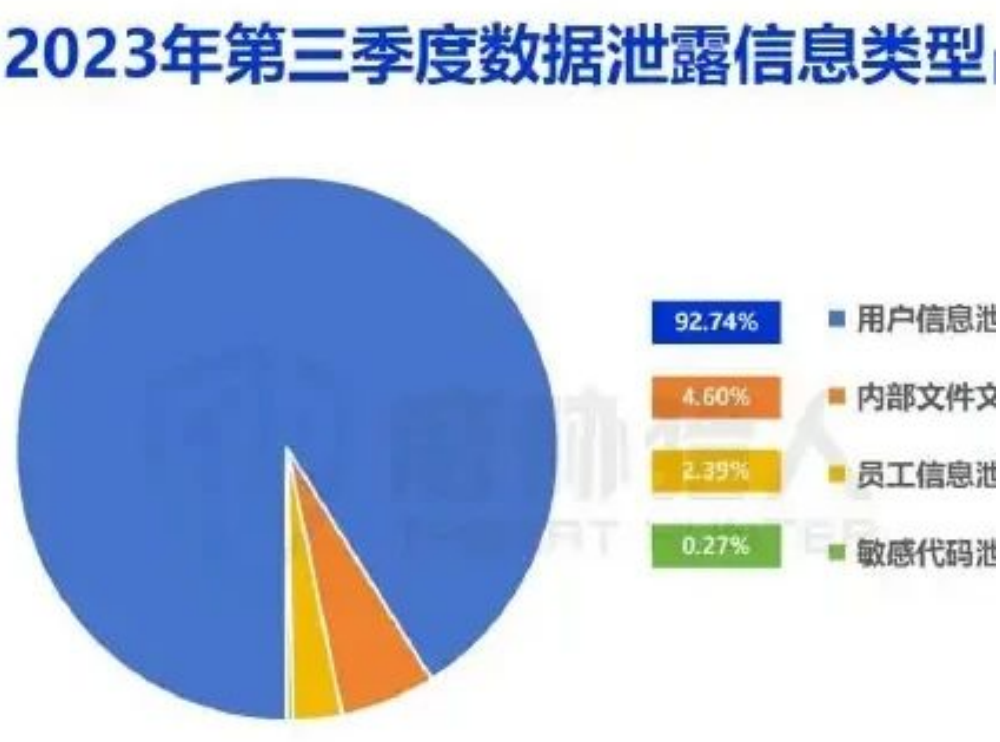
This situation will significantly increase the probability of financial platform users encountering fraud, which will cause them to be under regulatory pressure. At the same time, it will also bring negative public opinion to the platform.

In response to the above malicious activity incidents, enterprises should promptly understand their malicious activity procedures and details, and establish specific fraud-control rules based on their own business scenarios. In addition, enterprises also need to realize that the confrontation with external threat actors is dynamic and continuous, so at this time, they can rely on third-party cybercrime ecosystem intelligence data to achieve:

(1) In the ongoing confrontation with external cybercrime ecosystem, timely perceive attack risks through multi-channel monitoring of the entire network, analyze and extract specific cybercrime ecosystem trends, malicious tools and other attack information, and carry out targeted defense in a timely manner.

(2) To launch a specific attack, cybercrime ecosystem must use basic attack resources, such as phone number, IP, email, etc. Threat Hunter uses the rich cybercrime ecosystem intelligence data to extract cybercriminal groups attack patterns and resource characteristics, match them with abnormal traffic in enterprise business, and quickly identify risks.

With the help of "intelligence" capabilities, enterprises can comprehensively and timely perceive the trajectory and trends of cybercriminal groups from a global perspective, accurately warn and output IOC intelligence of attackers, and then link fraud-control systems, WAF, etc. to quickly deal with attack risks. Facing the increasingly severe cybercrime ecosystem risk challenges, we must respond calmly and fight back forcefully.

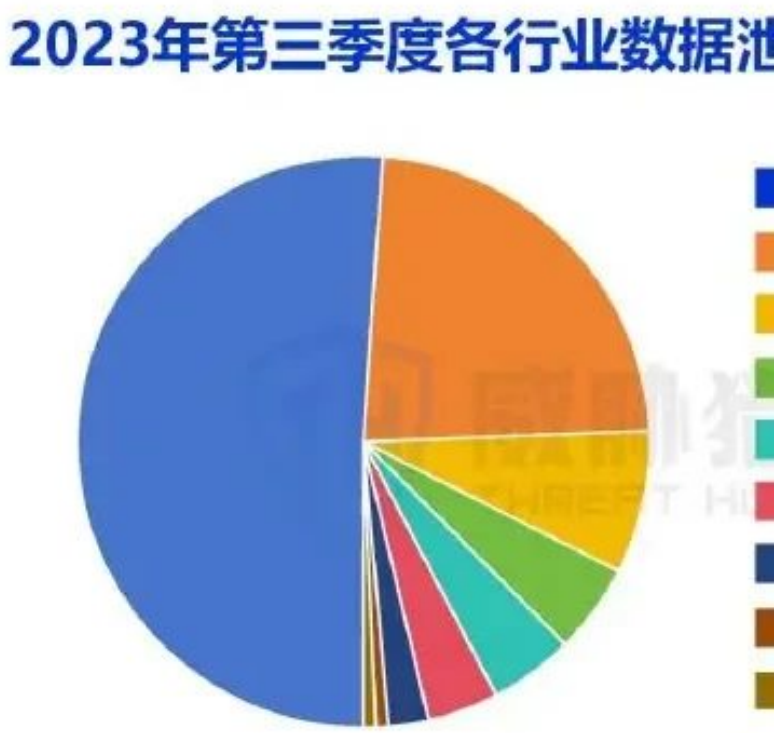


Data leaks in the third quarter cover a wide range of industries and the financial and logistics sectors remain the most affected areas (figure 1)

Source: Threat Hunter original report, page 29

English figure labels

1	Nose pointy.
2	= Internal
3	= employee information



Data leaks in the third quarter cover a wide range of industries, and the financial and logistics sectors remain high-risk areas (figure 2)

Source: Threat Hunter original report, page 29

English figure labels

1	One day.