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.

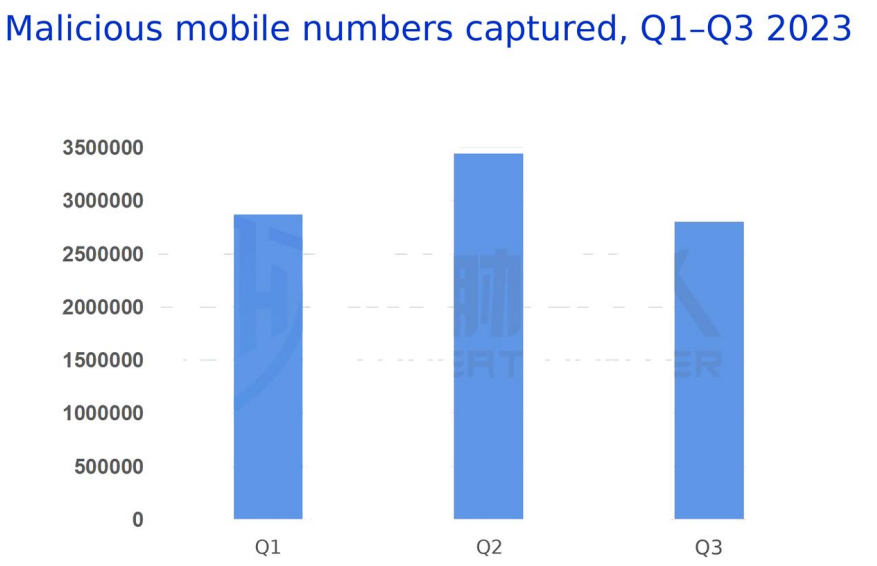
Analysis of attack resources used by cybercriminal groups in the third quarter of 2023

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.

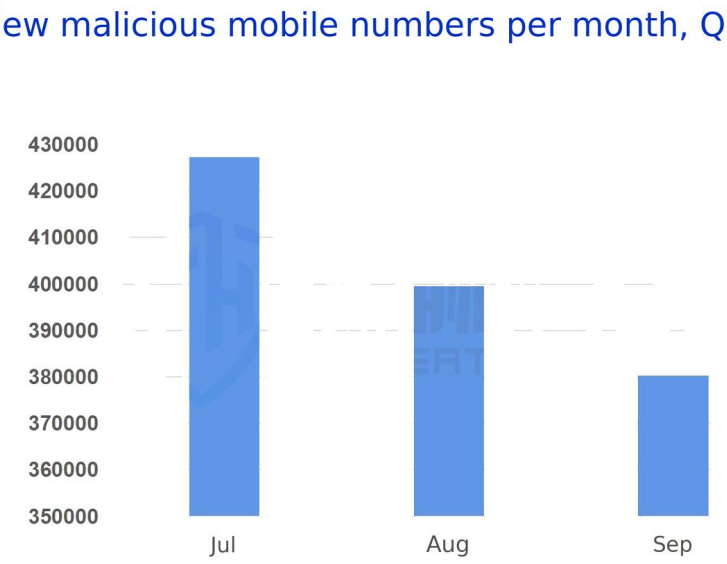


Malicious mobile numbers captured by Threat Hunter in each of the first three quarters of 2023

Source: Threat Hunter original report, page 5. Original figure with Chinese text replaced by English.

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.

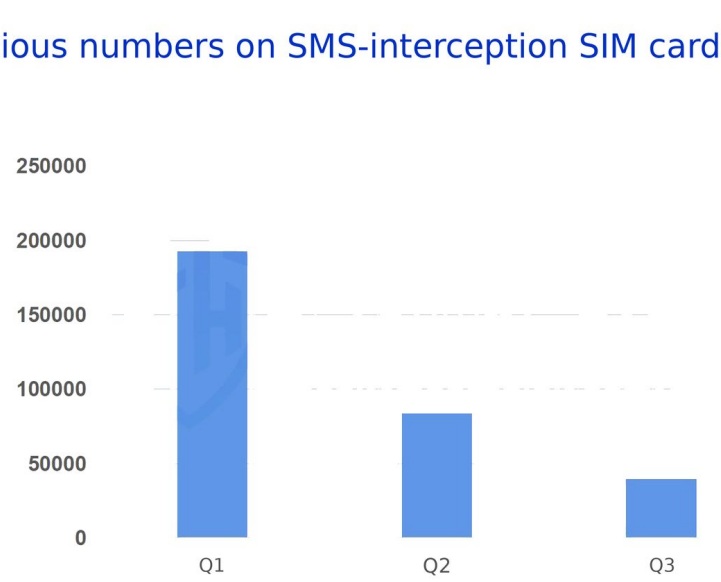


New malicious mobile numbers captured each month in Q3 2023

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

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.



New malicious numbers on SMS-interception SIM cards, Q1–Q3 2023

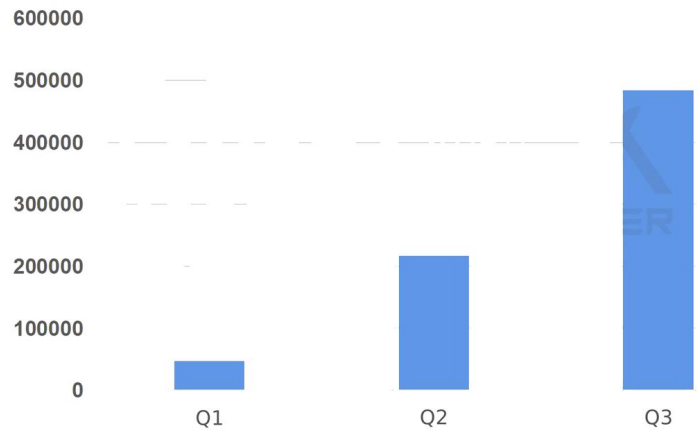
Source: Threat Hunter original report, page 6. Original figure with Chinese text replaced by English.

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.

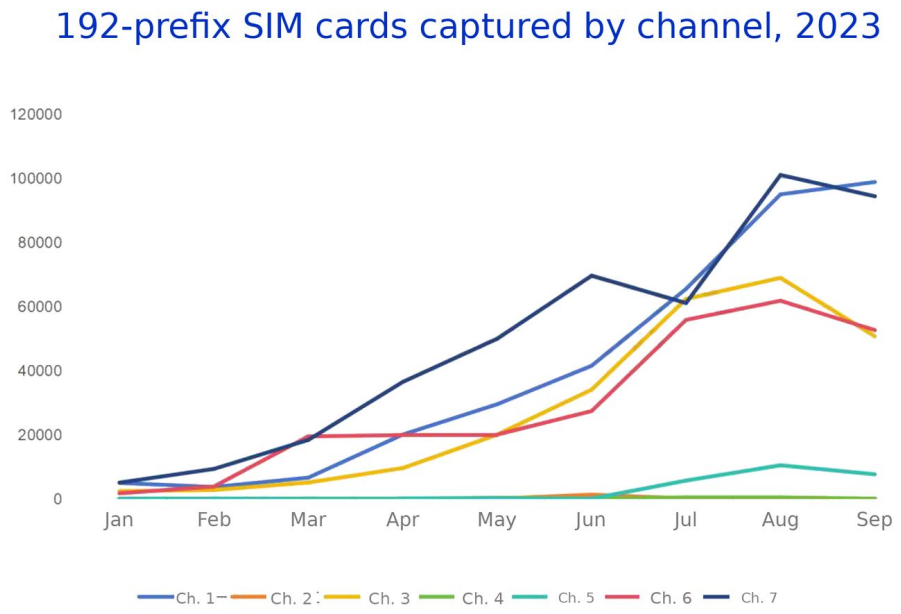
Malicious numbers in the 192 prefix captured, Q1–Q3 2023



Malicious numbers in the 192 prefix captured, Q1–Q3 2023

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

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 illicit SIM-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.



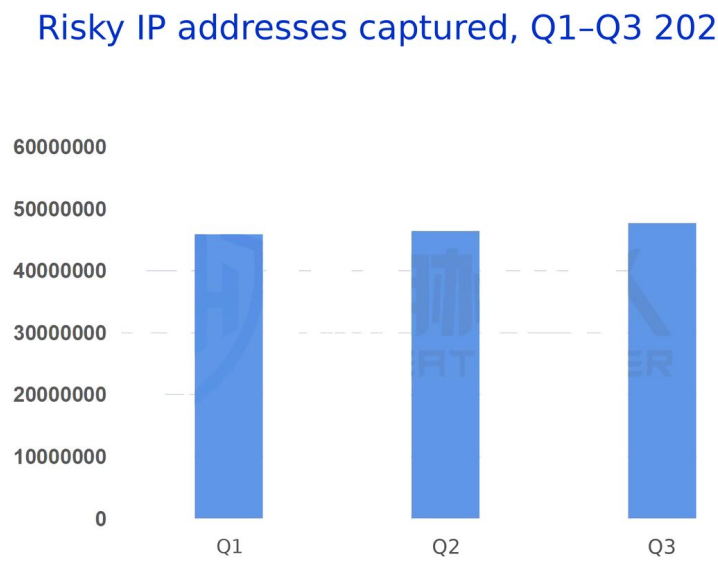
192-prefix SIM cards captured by channel, January–September 2023 (channels anonymised as in the original)

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

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.



Risky IP addresses captured, Q1–Q3 2023

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

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.

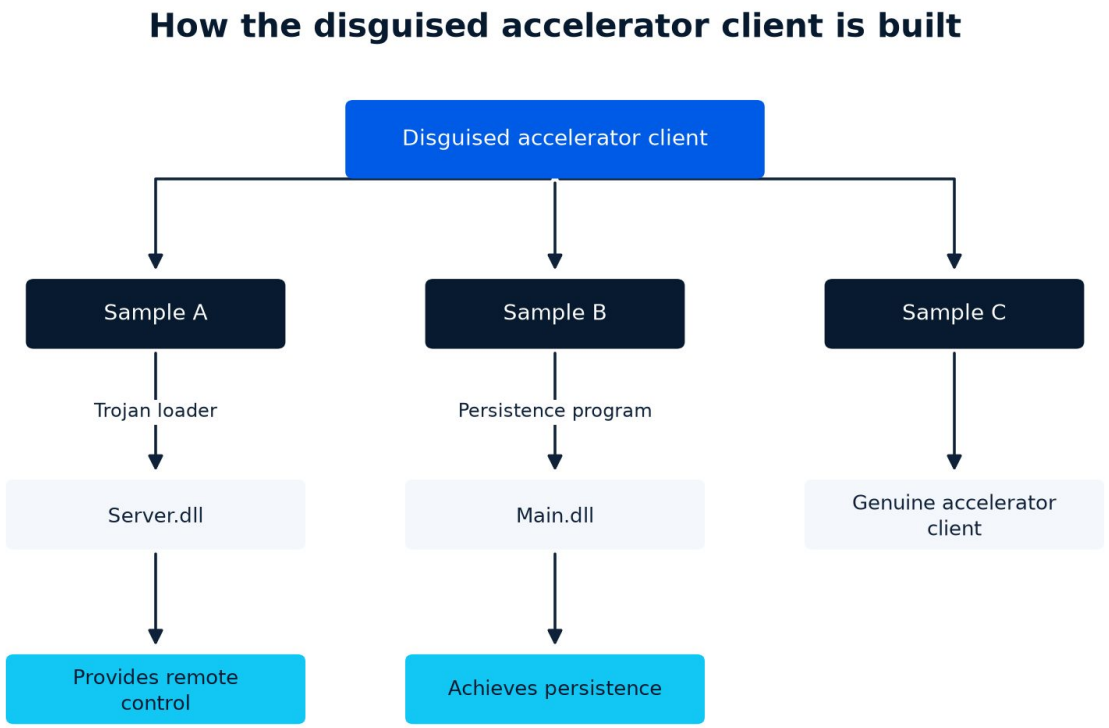
Taking the captured "xx accelerator" tool as an example, its malicious process is:

(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.



Structure of the disguised accelerator client: two malicious samples (a Trojan loader and a persistence program) bundled with the genuine client

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

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.

Function	Description
Function 1	Decrypts binary data, then loads the decrypted PE code into the process space through in-memory loading.
Function 2	A manual dump of the decrypted binary data shows that it is a DLL: a remote-control DLL from the Farfli Trojan family, with the full functionality of a remote-access Trojan.

Functions of Sample A

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

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.

Function	Description
Function 1	Decrypts the C2 address hackerXXXXXX.XXXXXX.net:8088. Before connecting from the victim's machine, it uses a mutex to check whether several instances are running, to avoid duplicate connections.
Function 2	Maintains the Trojan's persistence. Method 1: creates a system service named GUpdate, sets the registry path and adds a description and service name disguised as a core system service. If this succeeds, persistence is in place, and the executable then exits. Method 2: fakes a system service hosted by svchost, creates a hidden desktop, and downloads and runs a program from the C2 address in its settings, again to achieve persistence.

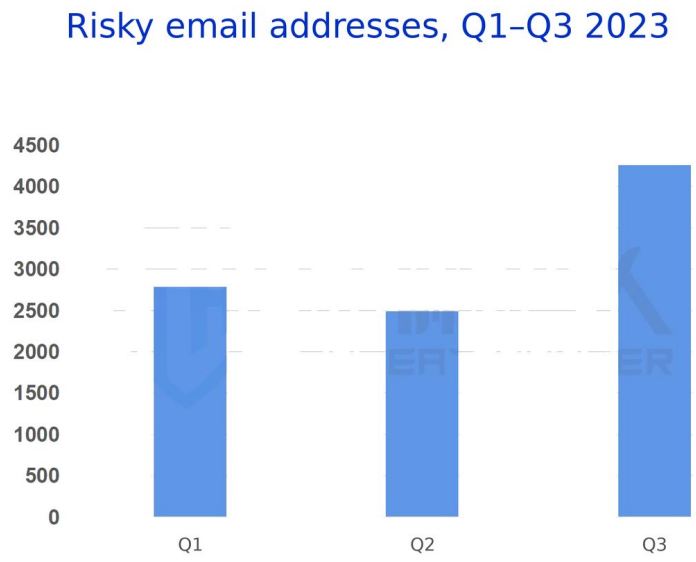
Functions of Sample B, including two ways it achieves persistence

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

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.



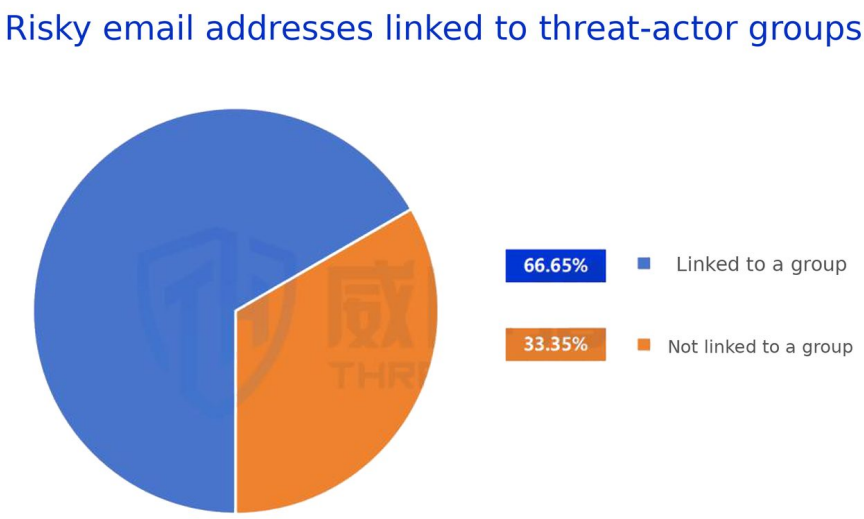
Risky email addresses captured, Q1–Q3 2023

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

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

Outside China, 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 businesses outside China.

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.



Share of risky email addresses that can be linked to threat-actor groups

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

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:

Strong association	Weak association
• The email domains resolve to the same MX record • The MX records resolve to the same IP address	• Same registrar, with very short intervals between registrations • Same name servers • Same registrant details

Features used to link email addresses to the same group: strong and weak associations

Source: Threat Hunter original report, page 12. Table re-typeset in English from the original.

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:

Group	Strong association: MX record of the email domains	Weak association: second-level domains	Weak association: registrant	Weak association: registration email	Weak association: name servers
Temporary-email group A (mailboxes 1–10,085)	All mail.***.kr	66 second-level domains, all in the format xxx.kr	Y**N	ax*****d@gmail.com	***.tad.cc, ***.tad.cc
(as above)	(as above)	nice***.com ho*****.com ba*****.com hig*****.com	ju****suk	***@naver.com	N***.HO***NG.CO.KR (all four)
(as above)	(as above)	sap*****lur.xyz	Not public	Not public	***.NS.CLOU***ARE.COM ***S.NS.CLOU***ARE.COM
(as above)	(as above)	ss*****ne.me	Not public	Not public	****.domai****trol.com (both)

"(as above)" marks a cell merged with the row above in the original. Masking (***) as in the original.

Example: association features of temporary-email group A

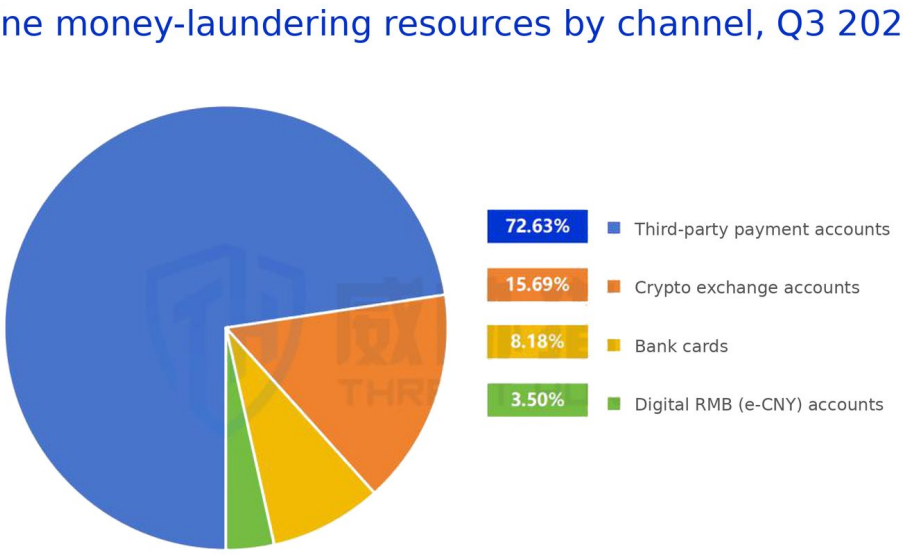
Source: Threat Hunter original report, page 13. Table re-typeset in English from the original.

1.4 Analysis of online money laundering resources in the third quarter

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.



Online money-laundering resources by channel, Q3 2023

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

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%.

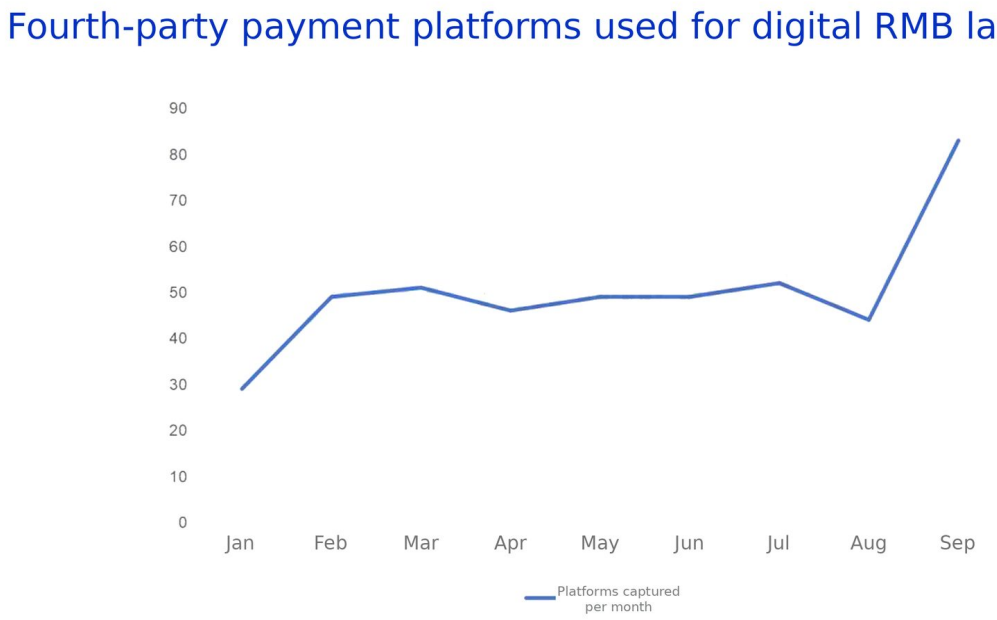


Digital RMB laundering records captured each month, April–September 2023

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

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.



Fourth-party payment platforms used for digital RMB laundering, captured each month in 2023

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

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.

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.



Corporate accounts used for laundering captured, Q1–Q3 2023

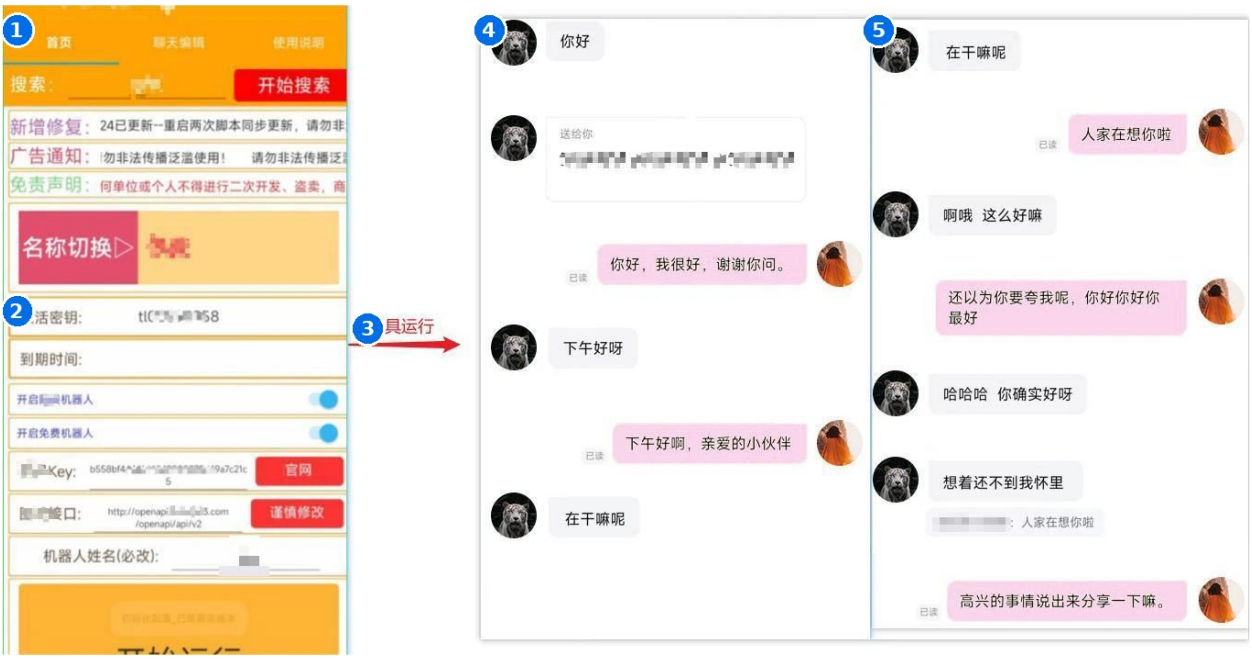
Source: Threat Hunter original report, page 16. Original figure with Chinese text replaced by English.

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.



An automatic chat tool connected to an AI robot: the settings panel (left) and the conversation it holds (right)

Source: Threat Hunter original report, page 18. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Settings panel of the automatic chat tool. Tabs: Home, Chat editor, Instructions; a search box with a "Start search" button. Notices: "New fix: updated on the 24th; restart the script twice to sync the update"; "Ad notice: do not spread illegally"; and a disclaimer forbidding any organisation or individual from redeveloping or reselling the tool
2	Settings: "Switch name"; activation key; expiry time; switches to enable the [redacted] robot and the free robot; the robot service's key and API endpoint (http://openapi.[redacted]5.com/openapi/api/v2) with "Official site" and "Change with care" buttons; "Robot name (must change)"; and a "Start running" button
3	Arrow: "Tool running"
4	Chat run by the robot (right-hand bubbles). Contact: "Hello". Robot: "Hello, I am fine, thank you for asking." Contact: "Good afternoon". Robot: "Good afternoon, my dear friend". Contact: "What are you up to?"
5	Chat, continued. Robot: "Thinking of you". Contact: "Oh, that's sweet". Robot: "I thought you were going to compliment me. You are the best". Contact: "Haha, you really are"; "Never thought you'd come to me". Robot: "Tell me something that made you happy."

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

	Preset scripts	AI robot
Feature 1	Only one social account per platform can be run: the scripts are fixed, so several accounts would send identical replies and trigger the platform's risk controls.	Several social accounts on the same platform can be run at once.
Feature 2	Each time the phone is changed, the script file has to be saved to the phone's storage directory.	Just enter the robot's API endpoint and key in the traffic-diversion tool.
Feature 3	Slow replies with fixed content.	Fast replies that read more like a real person.

Preset scripts compared with an AI robot in traffic-diversion tools

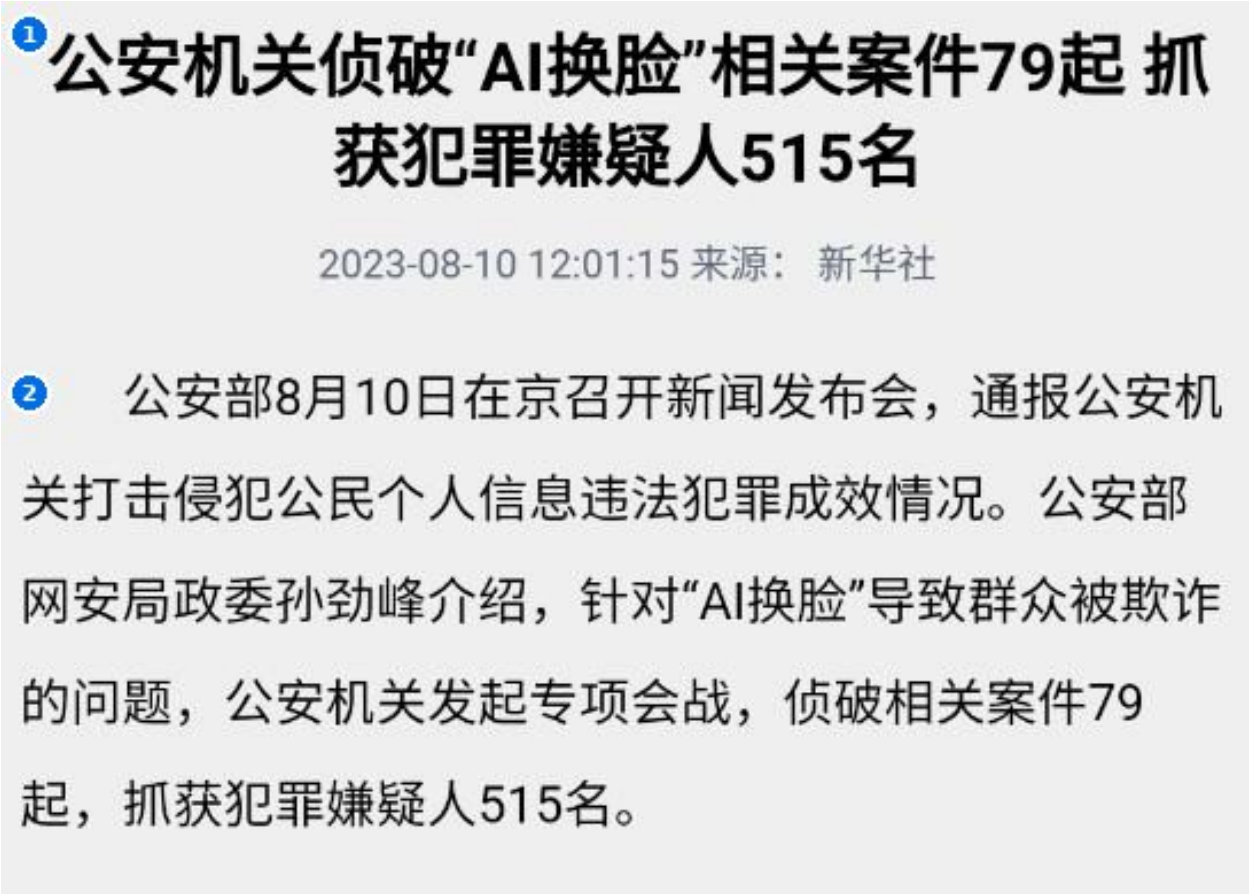
Source: Threat Hunter original report, page 19. Table re-typeset in English from the original.

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.



News report: police crack 79 cases involving AI face-swapping (August 2023)

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

Figure guide

1	Headline: "Police crack 79 cases involving 'AI face-swapping' and arrest 515 suspects" (10 August 2023, 12:01:15; source: state news agency)
2	"On 10 August the Ministry of Public Security held a press conference in Beijing on the results of the crackdown on crimes that infringe citizens' personal information. The political commissar of the ministry's Cybersecurity Bureau said that, in response to people being defrauded through 'AI face-swapping', police launched a special campaign, cracked 79 related cases and arrested 515 suspects."

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

Tool type	What it does
AI face-swap software	Trains a face-swap model on images or videos of the target taken from several angles, and outputs the trained model and face-swapped videos.
Real-time AI face-swap software for live streaming	Uses the model from the face-swap software to replace the streamer's face with the target's face in real time during a live stream, and outputs a preview window.
Video recording and live-streaming software	Feeds the preview window into a virtual camera as its video source for live streaming or video conferencing, or pushes the stream over RTMP to a specified server for live streaming.

Tools used for AI face-swap attacks and what each one does

Source: Threat Hunter original report, page 20. Table re-typeset in English from the original.

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.



Threat Hunter test, first attempt: logging in to the victim's bank account with the tester's own face fails face verification

Source: Threat Hunter original report, page 20. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Caption: "The tester uses their own face to log in directly to the victim's bank account"
2	Caption: "Face verification failed; login unsuccessful"

(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.



Threat Hunter test, second attempt: an AI face-swap video of the victim passes the bank app's face verification

Source: Threat Hunter original report, page 21. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Caption: "The tester makes an AI face-swap video of the victim and, by a specific method, makes the video's footage the image the login device's camera captures"
2	Caption: "Logs in with the victim's AI face-swap video, triggering face verification"
3	Caption: "Face verification passed; login successful"

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.

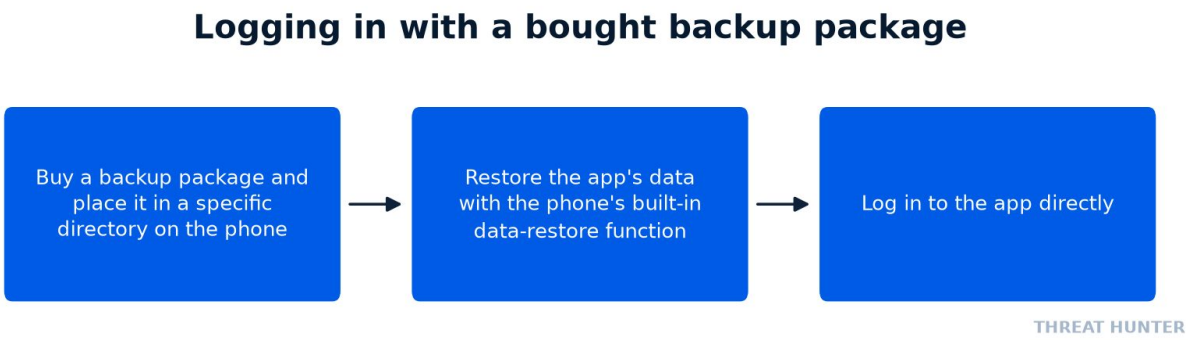
The following is how some threat actors use malicious activity accounts organized by Threat Hunter:

Account type	Description	How it is logged in
Password account	Login ID plus password; the most common way to log in.	Log in directly with the account and password.
Contacts-list account	Some apps can verify a login through the phone's contacts list. When selling an account and password, some threat actors also supply a contacts file ("vps file").	The threat actor imports the file on the attack device, logs in with the account and password, and chooses contacts-list verification when a login check appears.
IMEI account	The IMEI is the phone's serial number, in effect its identity card. Threat actors who register accounts usually sell each account together with the IMEI of the phone it was registered on.	The attacker changes the phone's IMEI with a specific tool so that the platform takes the attack device for a trusted (not new) device; logging in with the account and password then avoids login verification.
Backup-file account	After registering an account, the threat actor uses a device-modification tool to back up the target app's account information, cache files and device parameters into one file.	With the backup file, the attacker restores it on the attack device using a device-modification tool, so that the platform takes the attack device for a trusted device that is already logged in.
Backup-package account	The phone's built-in backup function is used to back up a specific app's data into a backup package.	After buying the backup package, place it in a specific directory on the phone, then log in through the phone's built-in data-restore function.

Types of hijacked account sold by threat actors, and how each is logged in

Source: Threat Hunter original report, page 22. Table re-typeset in English from the original.

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

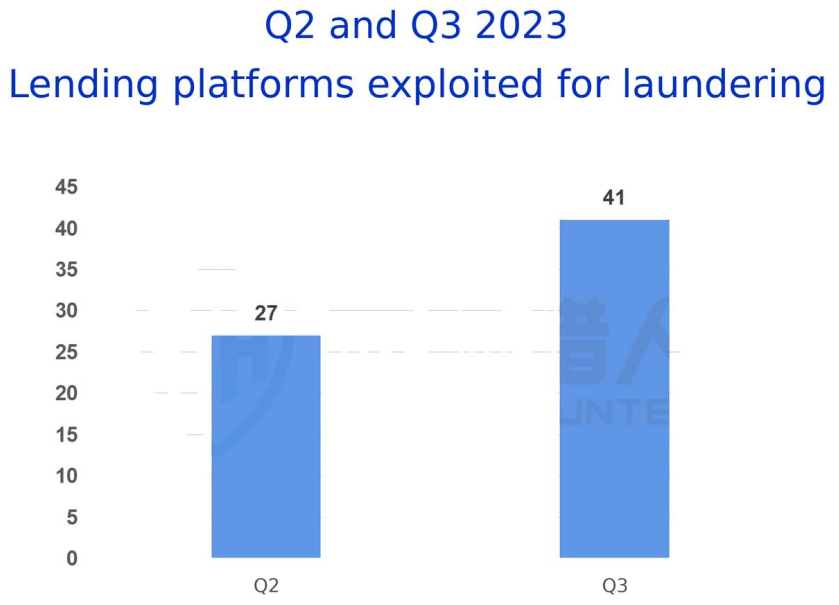


How a backup-package account is used to log in to a social app

Source: Threat Hunter original report, page 22. Redrawn in English from the original figure.

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.



Lending platforms exploited for laundering, Q2 and Q3 2023

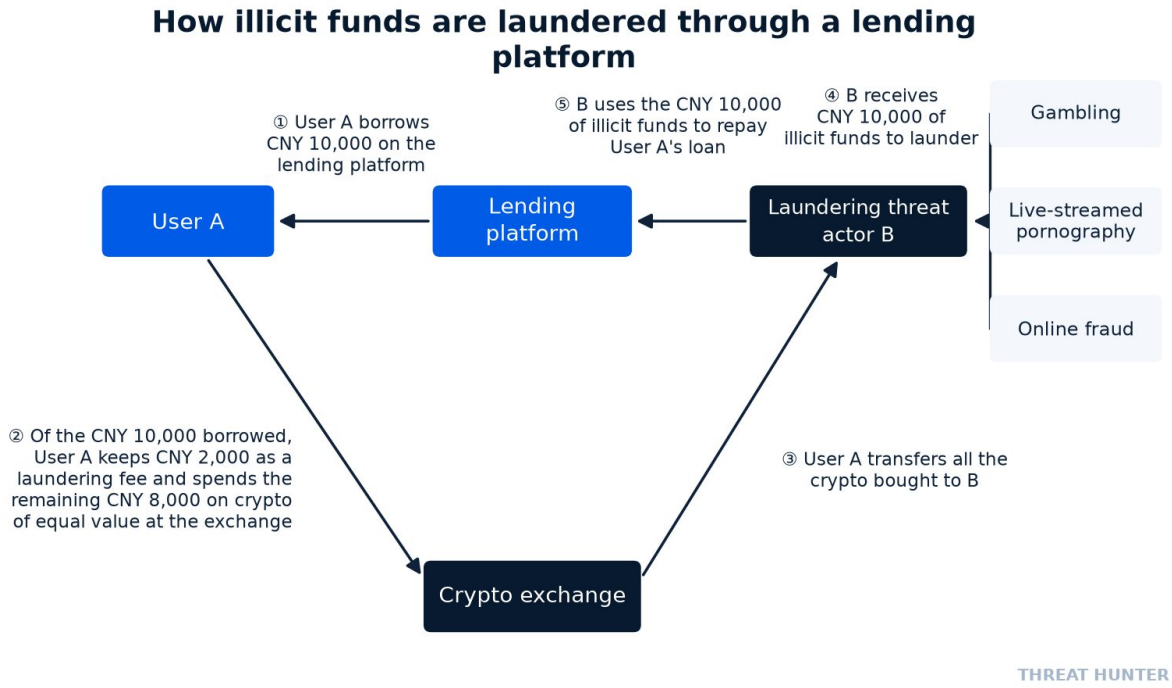
Source: Threat Hunter original report, page 23. Original figure with Chinese text replaced by English.

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.

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:



How illicit funds are laundered through a lending platform, a borrower and a crypto exchange

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



Chat with a laundering platform's promoter: selling USDT to "repay" a small loan, and the app's order-grabbing screens

Source: Threat Hunter original report, page 24. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Q (10:18): "Hi, can you explain what moving USDT ('U') in the group actually means?"
2	A (10:41): "[Redacted] is a crypto trading platform: upstream it connects to U merchants, downstream to trading users. If you have U (if not, you can buy it on other exchanges), just sell it on [redacted]; U merchants on [redacted] buy U at a high price. The platform uses a two-way escrow model to secure both sides' funds, and after a trade it charges only 2% of the trade amount as a platform fee."
3	Q (10:46): "So how do the 'matching' and 'order grabbing' in the group work?" A (10:47–10:48): "Order grabbing is when you take orders yourself: enter the amount to sell and you get paid, all in one payment." "Matching: once you turn it on, orders are matched automatically." "The amount credited isn't fixed; it may arrive in several payments within your sale range."
4	Video of the app's "Task hall": tabs "Order grabbing centre" and "Matched orders"; orders of 100,000 USDT at CNY 7.6 and 500,000 USDT at CNY 7.5 per unit, each with a "Grab" button. Subtitles: "Task hall – choose Matched orders – tap Auto-grab" and "Task hall – Order grabbing centre – tap Grab (grab orders yourself)"
5	Q (10:53): "So with both order grabbing and matching I sell U to you? You buy U and pay money into my bank card?" A (10:55): "Not to us; [redacted] is just an escrow trading platform." A (10:56): "Once you turn on matching, U merchants can see your sale amount and payment details, and pay the amount they need into your receiving card."
6	Q (10:58): "Oh, I see. The group also said you can go after small-loan platforms. How does that work?" A (11:01): "By repaying your small loan for you. Say you owe CNY 50,000 on a [redacted] loan: you only need to sell 6,411 U to the merchant (6,411 × 7.8 = 50,000). After the sale, the U merchant pays CNY 50,000 into the small-loan company's account to repay your loan, while the 6,411 U you bought with the CNY 50,000 you borrowed costs only 44,877 at the market price of 7. 50,000 − 44,877 = 5,123 is your profit."
7	Q (11:04): "Oh, what do I need to register for your app?" A (11:04): "Nothing."

The final result of this money laundering method is:

Party	Outcome
User A	Earns CNY 2,000 by helping others launder money.
Laundering threat actor B	Gives up 20% of the funds to turn illicit money into cryptocurrency, which is subject to less monitoring.
Lending platform	Is exploited by the launderers: illicit money arrives in its corporate account.

What each party gains or loses in loan-platform laundering

Source: Threat Hunter original report, page 25. Table re-typeset in English from the original.

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:

Platform	iOS cloud phone price	Apps installable via App Store or i4 Assistant?	Jailbroken device?	Jailbreak plug-ins installable?	Built-in device modification?
Platform 1	CNY 88/month	Yes: through both the App Store and i4 Assistant	Yes	Yes: installed directly with no platform review (e.g. Zorro)	Yes
Platform 2	CNY 77/month	Yes: through its own app market	Not yet determined	Not yet determined	No
Platform 3	iPhone 8: CNY 88/month iPhone 8 Plus: CNY 108/month iPhone SE 2: CNY 138/month	Yes: through both the App Store and i4 Assistant	Yes	Yes, but plug-ins must first pass platform review	No
Platform 4	CNY 77/month	Yes: through both the App Store and i4 Assistant	Yes	Yes, but plug-ins must first pass platform review	No

iOS cloud phones offered by four platforms: prices and capabilities

Source: Threat Hunter original report, page 25. Table re-typeset in English from the original.

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 smartphone 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.

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.

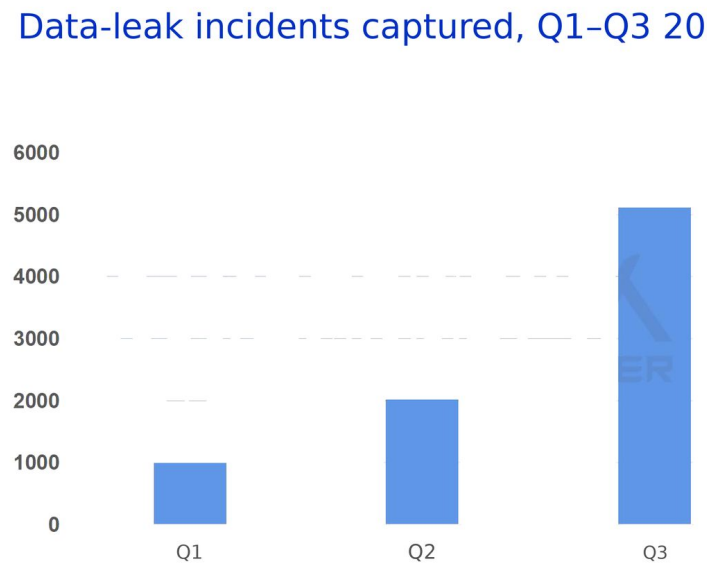
In response to such situations, Threat Hunter recommends that companies should obtain samples of such platforms in a timely manner and conduct relevant sample analysis and defense.

Analysis of data breach scenarios in the third quarter of 2023

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

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.

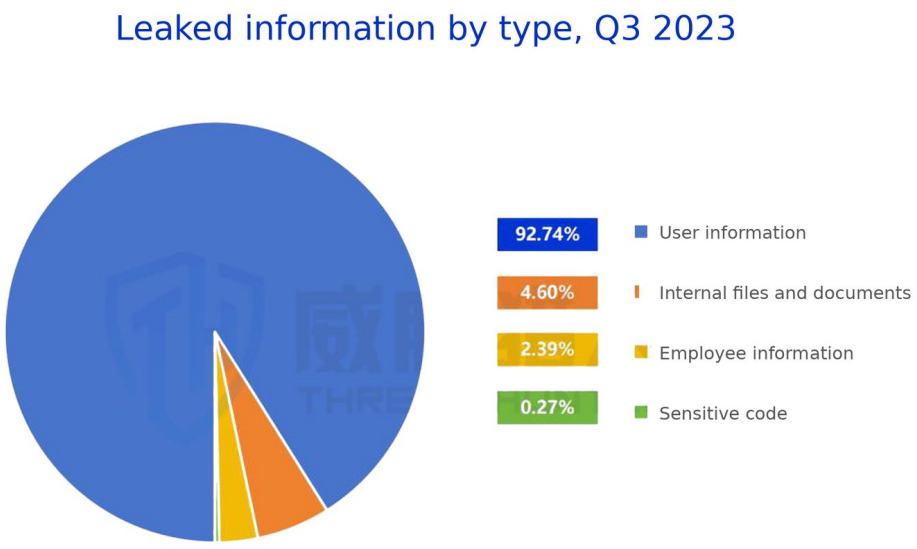


Data-leak incidents captured, Q1–Q3 2023

Source: Threat Hunter original report, page 28. Original figure with Chinese text replaced by English.

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.

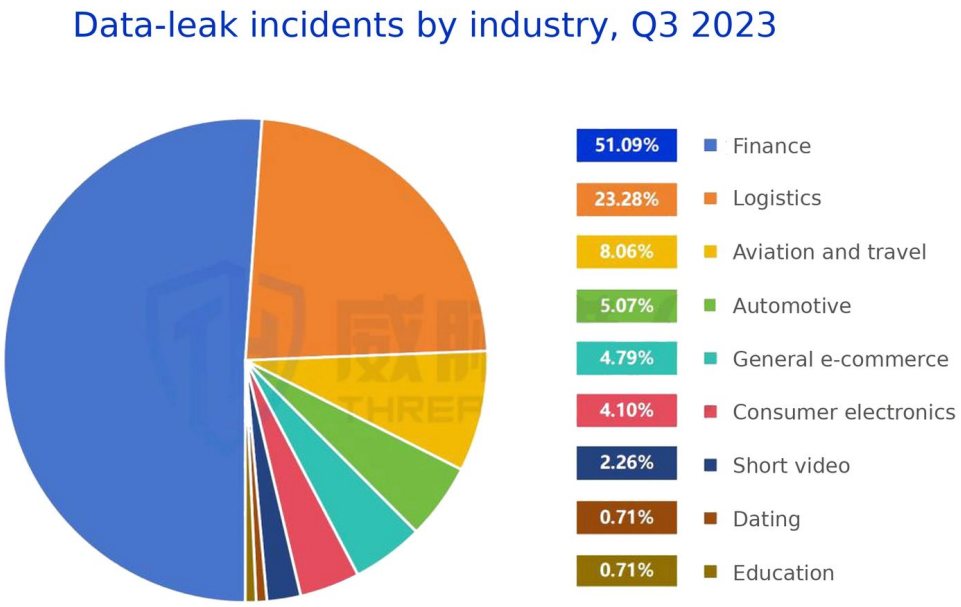


Leaked information by type, Q3 2023

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

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.

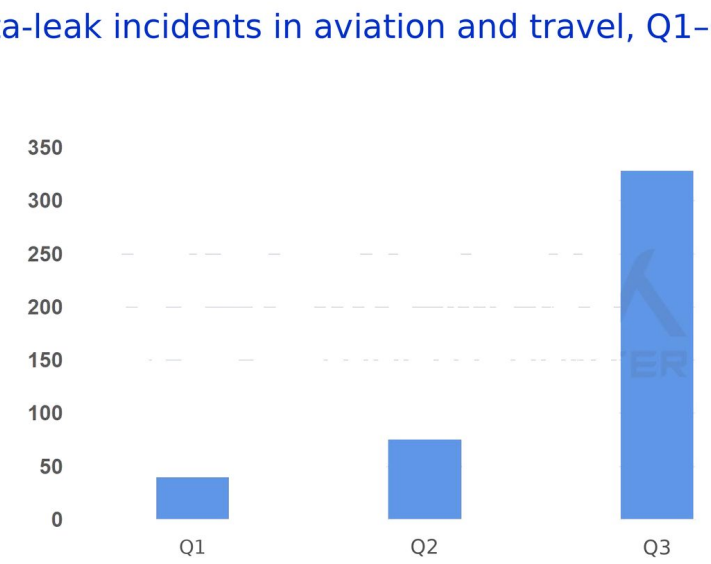


Data-leak incidents by industry, Q3 2023. Shares as published; they sum to 100.07% because of rounding.

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

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%.



Data-leak incidents in the aviation and travel industry, Q1–Q3 2023

Source: Threat Hunter original report, page 30. Original figure with Chinese text replaced by English.

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

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 a major encrypted messaging app 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.



Threat Hunter alert: employee email addresses of a financial investment company offered in a messaging-app data-trading group (August 2023)

Source: Threat Hunter original report, page 31. Original image retained; numbered translations added by Threat Hunter.

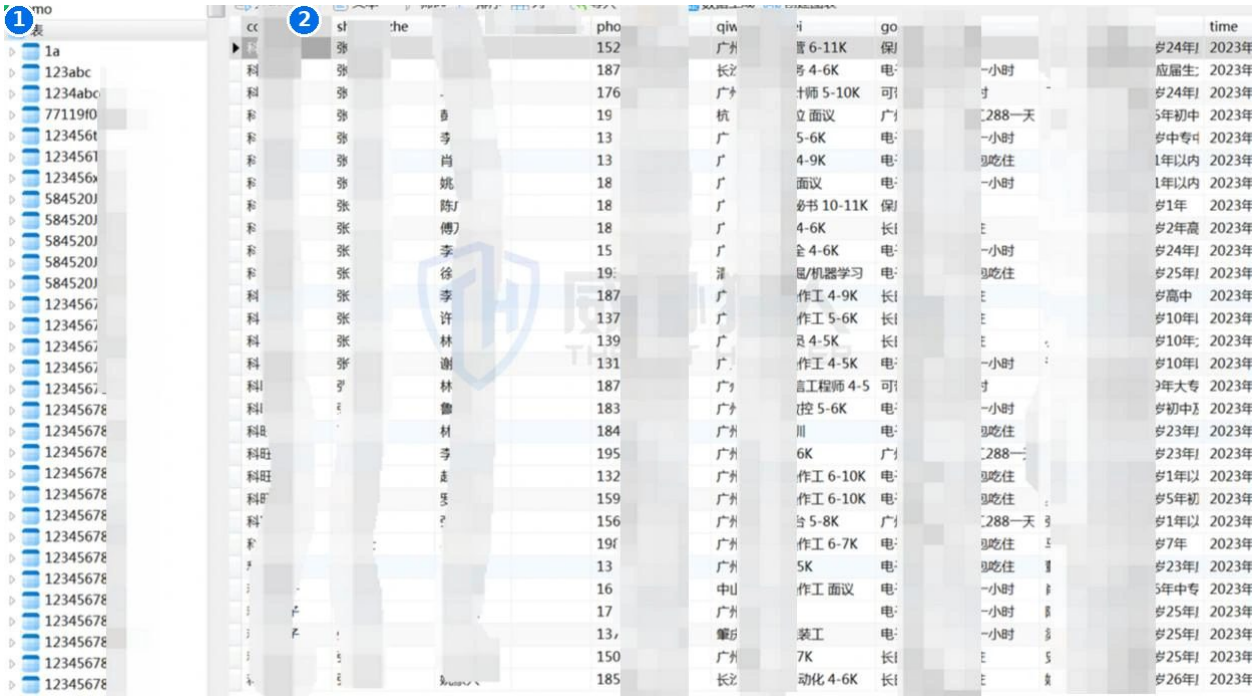
Figure guide

1	Alert title: "Sensitive information about '[redacted]' posted by threat actors captured in the messaging-app underground data-trading group '[redacted]'". Category: data leak; type: employee information leak. Buttons: pending, request takedown, feedback, export PDF
2	Risk overview: discovered 2023-08-24 15:04:35; data volume: unknown; sale price: unknown; cause of leak: suspected Trojan or virus attack; data format: email addresses; authenticity: cannot be verified ("[redacted] specific customer internal verification data"); historical data: cannot be verified
3	Risk details: data sample

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.



Resume data crawled from a recruitment website and stored on a third-party platform's server

Source: Threat Hunter original report, page 32. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Database "demo" on the third-party platform's server: the list of tables on the left
2	Rows of crawled resumes. Columns include company, name, phone number, city, desired job and salary (e.g. 4–6K, 5–10K) and other resume fields such as commute, age, education and date; personal details are blurred

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.

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.