THREAT HUNTER RESEARCH

Fraud in the Mini Program Ecosystem

A study of fraudulent registration, promotion abuse and automated attacks across the mini program ecosystem.

Original publication: 2021-09-08
Research team: Threat Hunter Research Team
Source report: 27 pages

Original report text

This text version is reconstructed based on the 27-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.

Table of Contents 1. Current status of the cybercrime ecosystem activities around mini programs

1.1. Attacks against mini programs are growing rapidly, and the attacks are mainly promotion abuse

1.2. Online businesses in traditional industries have become the hardest hit area by attacks, with attacks spread across all walks of life

1.3. Mini-program attack costs are low and the attack is easy to scale

1.4. There are many ways to make money, and cash red envelopes are the most favored by cybercrime ecosystem

1.5. The cybercrime ecosystem around mini programs has formed a mature industry chain

2. Analysis of the cybercrime ecosystem chain of mini programs

2. 1. Upstream of the industrial chain

2. 2. Midstream of the industrial chain

2. 3. Downstream of the industrial chain

3. Analysis of Mini Program Attack Cases

3.1. The one-yuan purchase activity of a certain financial service platform was attacked

3.2. The cash activities of a certain life service platform were attacked

3.3. The rush buying activity of a certain brand of tea beverage company was attacked

4. Difficulties in attack and defense of mini programs and protection ideas

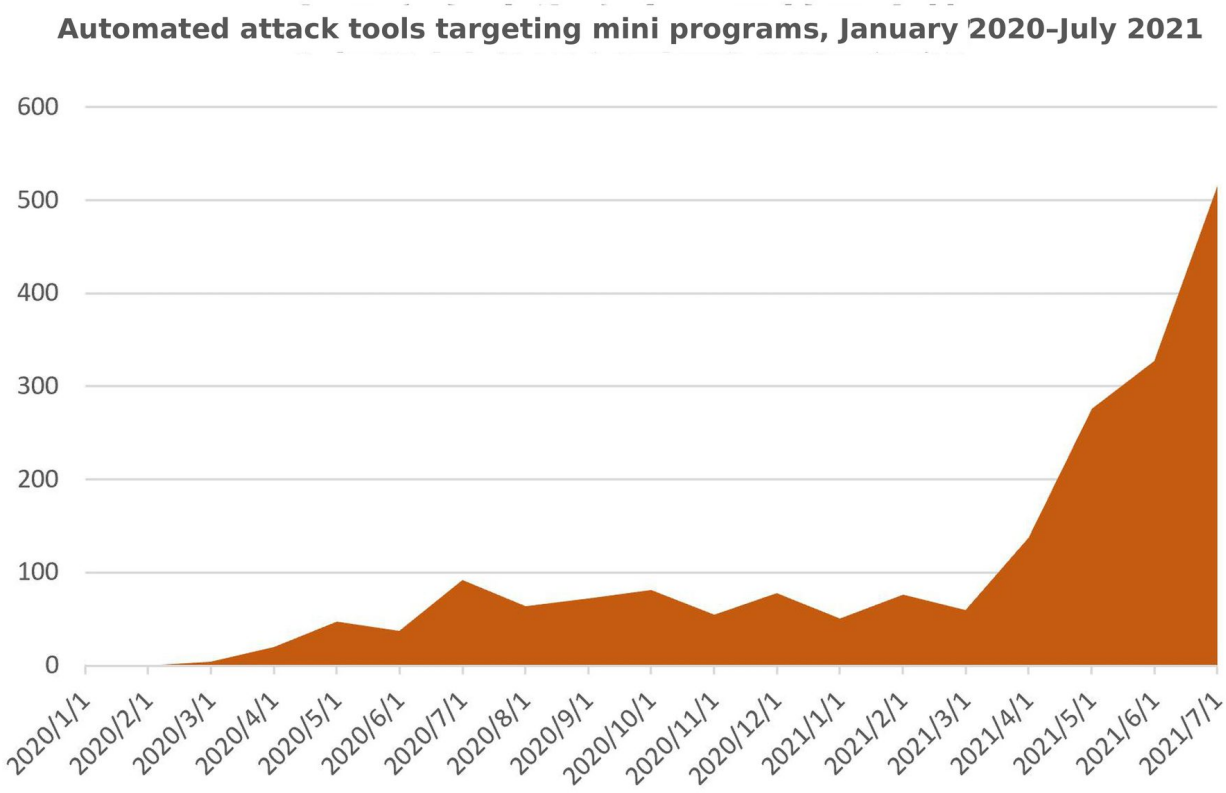
4. 1. Difficulties in attacking and defending mini programs

4. 2. Protection ideas for mini programs

1. Current status of the cybercrime ecosystem activities around mini programs

1.1. Attacks against mini programs are growing rapidly, and the attacks are mainly promotion abuse.

With the rapid growth of mini programs themselves and the maturity of the cybercrime ecosystem chain attached to mini-programs, attacks against mini-programs have also shown a rapid growth trend. Based on the cybercrime ecosystem tool data captured by the Threat Hunter business security intelligence platform, we have calculated the trend in the number of mini program automated attack tools from January 2020 to the present, as shown below:



Automated attack tools targeting mini programs, January 2020–July 2021: a steep rise from early 2021

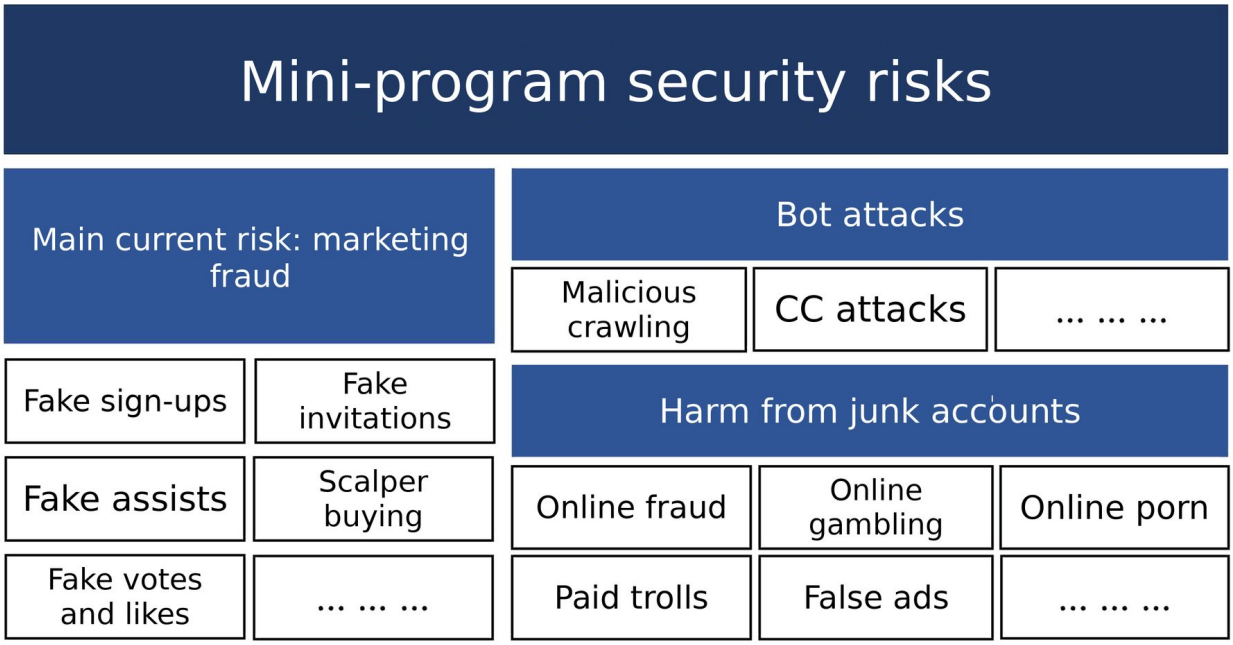
Source: Threat Hunter original report, page 3. Original figure with Chinese text replaced by English.

The emergence of a large number of automated attack tools, on the one hand, shows that mini programs have brought enough benefits to cybercrime ecosystem, so that professional cybercriminal groups are willing to invest resources and technology; on the other hand, it also shows that the current security of mini programs cannot effectively block or limit cybercrime ecosystem, thus leading to the activity of cybercriminal attacks.

The current attack targets are mainly marketing activities carried out by enterprises on mini programs, through false registrations, false invitations, and scalpers.

fraud through panic buying and other methods has caused losses in marketing expenses and at the same time, corporate business has not achieved healthy growth. In the long run, automated attacks (also known as BOT attacks) will also bring more security risks, including malicious

crawling of enterprise data/user data, interface traffic manipulation, CC attacks causing service unavailability, etc. The influx of a large number of spam accounts will also cause huge damage to the platform's ecology, including the spread of illegal activities such as online pornography, online gambling, and online fraud, the manipulation of public opinion by online trolls, and the release of false advertising.

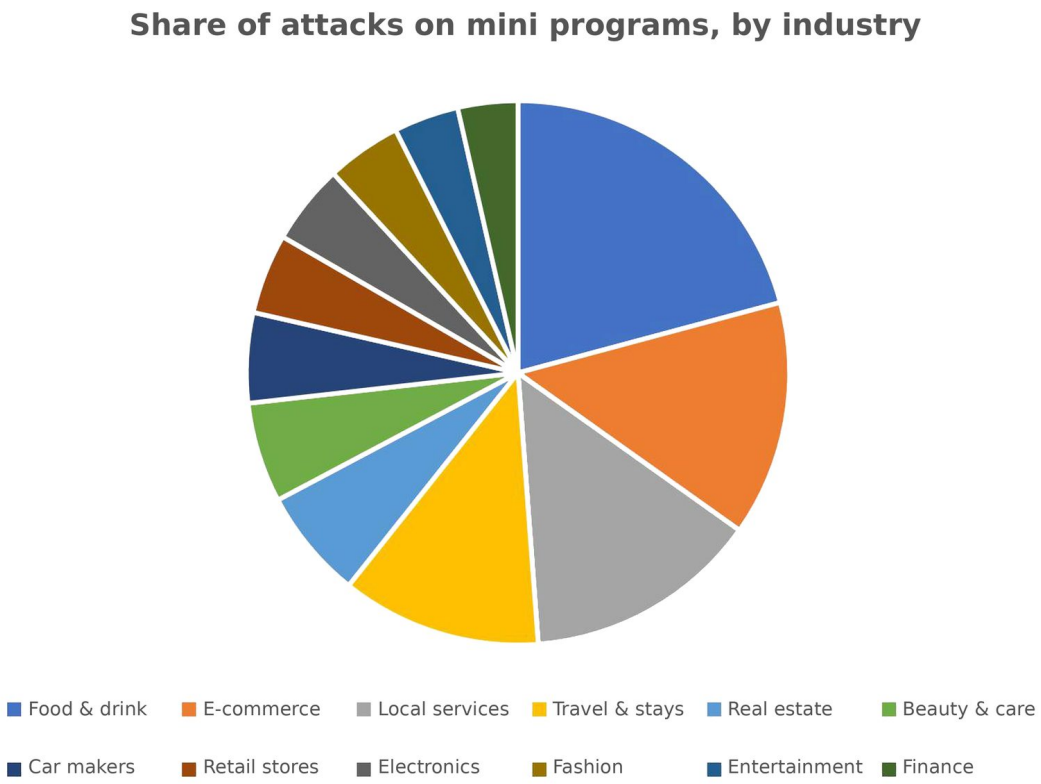


Mini-program security risks: marketing fraud today, plus bot attacks and harm from junk accounts

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

1.2. Online businesses in traditional industries have become the hardest hit area by attacks, with attacks spread across all walks of life.

Relying on a super app, mini programs have natural advantages in terms of convenience, stability, and user reach. This makes mini programs the first choice for many traditional industries to expand their business from offline channels to online services, and has played a huge role. On the other hand, these companies relatively lack understanding of cybercrime ecosystem and experience in offensive and defensive confrontation. Therefore, while enjoying the dividends brought by mini programs, they have also become key targets of cybercriminal attacks. Based on data from the Threat Hunter business security intelligence platform, we divided the attacked mini programs by industry and calculated the proportion of attacks, as follows:



Share of attacks on mini programs, by industry: food and drink is the most attacked

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

It can be seen that attacks are spread across all walks of life that are closely related to our lives. We selected some industries to make a brief inventory.

Food and catering: "Food is the first priority for the people." The traditional food and catering industry, represented by wine, beverages, refreshments, snacks, etc., has expanded from offline channels to online services with the help of mini programs to provide customers with more convenient and better services. However, it has also been targeted by the cybercrime ecosystem and has become the industry most attacked by the cybercrime ecosystem. Attacks on mini programs in the food and catering industry mainly include free orders, coupon grabbing, flash sales, etc.

E-commerce shopping: E-commerce shopping has always been a key industry for cybercriminal attacks. In addition to the leading Internet e-commerce platforms, some e-commerce platforms built by traditional enterprises have also emerged in the mini program ecosystem. These platforms often conduct social marketing and consumption through business models such as group buying, price bargaining, and point redemption. However, this business model has been familiar and exploited by the cybercrime ecosystem, and the profits of merchants are often captured by the cybercrime ecosystem.

Life services/travel accommodation: Internet services have covered all aspects of our lives and travel, ranging from takeout, express delivery, taxis, and hotels to marriage, education, medical care, and elderly care. There are both large and small Internet companies, as well as non-interactive enterprises undergoing digital transformation, as well as online services developed by the government to improve the quality of residents or attract tourists.

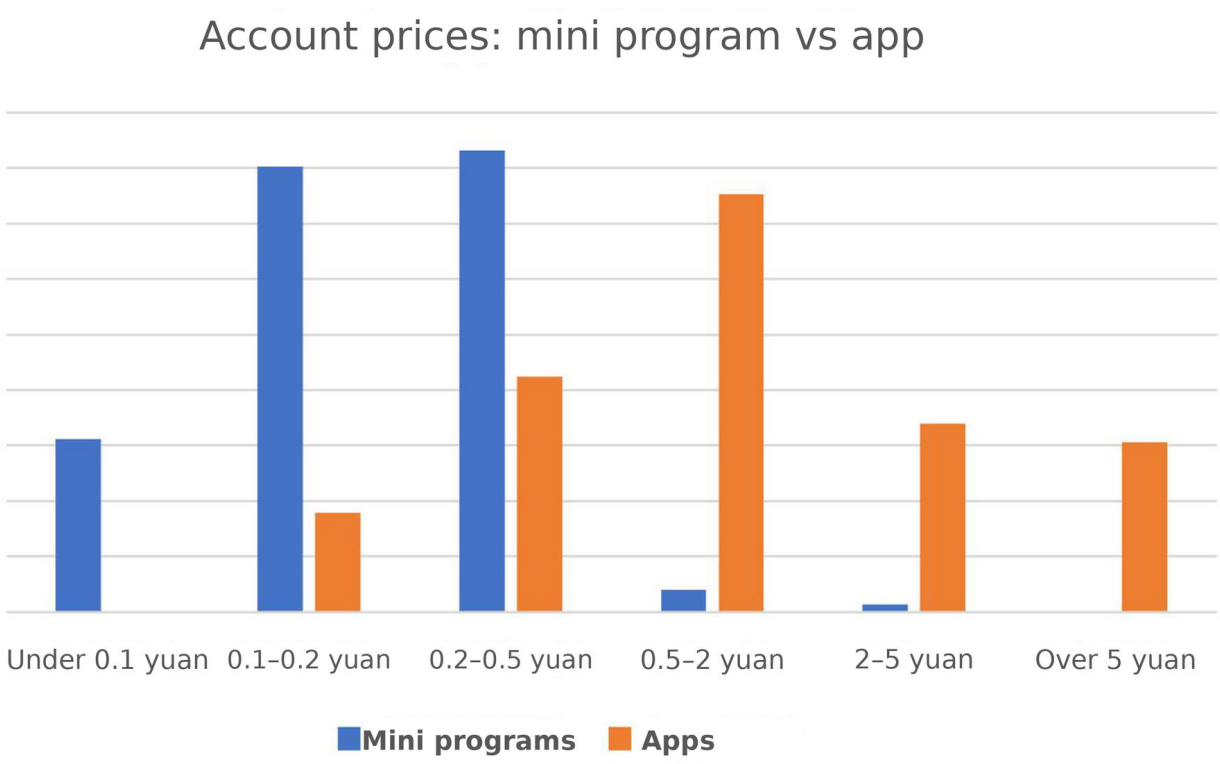
While ordinary people have gained convenience in their lives, cybercriminal groups have also gained benefits from it.

Real estate/automobile manufacturing: Real estate and automobile manufacturing can be said to be very typical traditional industries. In the wave of digital transformation, these companies use mini programs to carry out their original businesses, such as viewing houses/cars, buying houses/cars, renting houses/cars, etc.; on the other hand, they also use mini programs to enrich and expand their business, such as providing owner/car owner services, holding welfare activities, etc. Among the welfare activities, there are some online activities to invite friends to help, and cybercriminal groups can easily profit from them.

Supermarkets/Digital Home Appliances/Clothes and Accessories/Beauty and Care: The biggest change in the digital transformation of these industries is the expansion of product sales from physical stores to online, including mini programs. Most companies tend to learn from e-commerce marketing ideas. For example, some well-known domestic and foreign sports brands, cosmetics brands, etc. will launch their own marketing activities during certain periods of time (holidays or e-commerce promotion days, etc.) to give users large enough discounts. These discounts in physical stores are given to customers who really want to shop, while these discounts online often fall into the hands of cybercrime ecosystem, such as scalpers and shoe speculators.

1.3. Mini-program attack costs are low and attacks can be easily scaled up.

Account resources and device resources are the main costs of cybercriminal attacks. Mini program accounts rely on super-app authorized login. The current selling price is only 0.1 to 0.5 yuan per account. In contrast, App accounts mainly rely on receiving SMS verification codes on mobile phones. The price is generally much higher, and the prices of some popular services are even more expensive (note: this is limited to the price comparison of single authorization/code reception, and does not include the sale of maintained accounts or old accounts).



Account prices: most mini-program accounts cost under 0.5 yuan, while most app accounts cost more

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

The larger the scale of cybercriminal attacks and the more accounts required, the more obvious the price advantage of mini programs in account resources will be.

In addition, according to the analysis of Threat Hunter-Guigu Lab security experts, the current attack tools against mini programs are almost all protocol attacks, and protocol attacks do not require mobile phones, group control and other equipment resources, so the cost of attacks is greatly reduced. Several common ways for cybercrime ecosystem to implement automated attacks are compared as follows:

Attack method	How it works	Needs devices
Protocol attack	Crack the API protocol and forge API requests directly	No
Simulated-operation attack	Write scripts with tools such as keystroke-macro apps or Auto.js that simulate operating the app interface; for web apps, web automation test frameworks such as Selenium can also be used	Yes
Injection and hook attack	Use frameworks such as Xposed or Frida to write plug-ins that are injected into the app and hook key code, then monitor or tamper with the app's internal data or execution flow	Yes

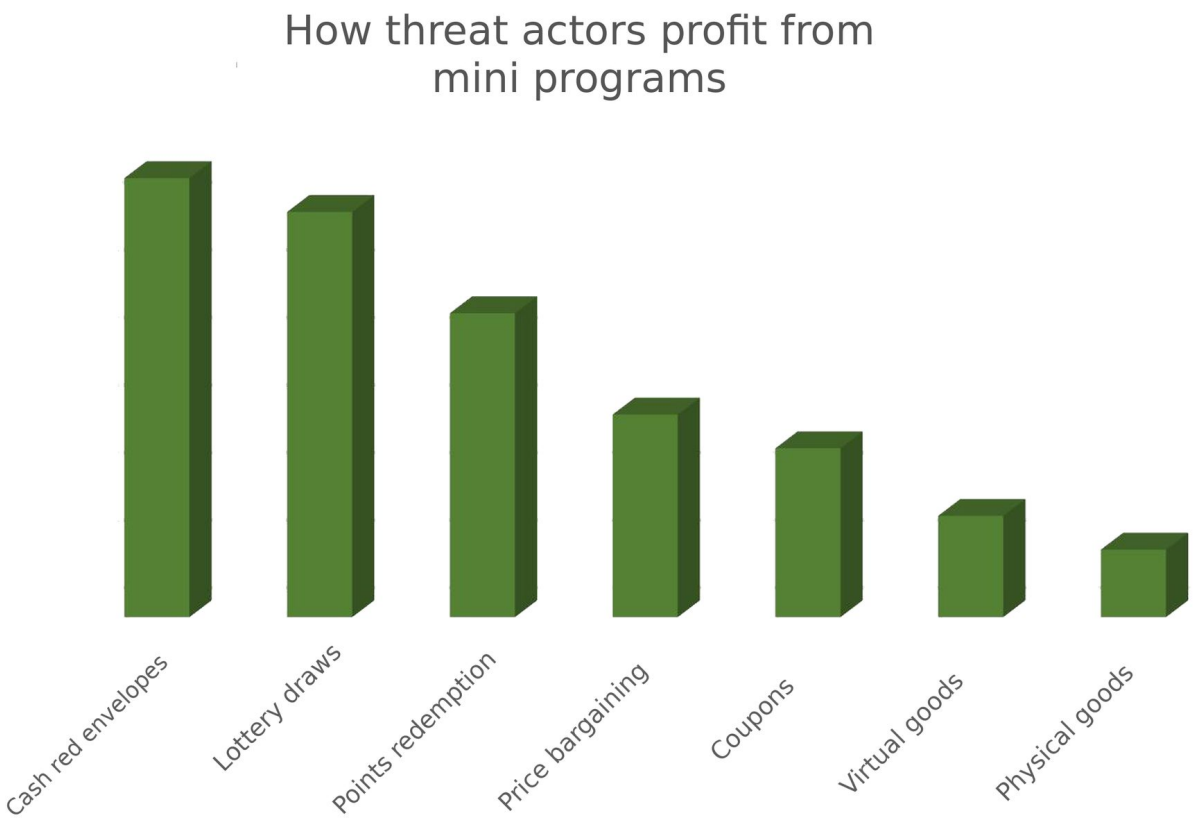
Common ways to automate attacks: protocol attacks need no devices

Source: Threat Hunter original report, page 7. Table re-typeset in English from the original.

Once beyond the limitations of the device, even a rudimentary cybercriminal group can easily carry out large-scale attacks.

1.4. There are many ways to make money, and cash red envelopes are the most favored by cybercrime ecosystem.

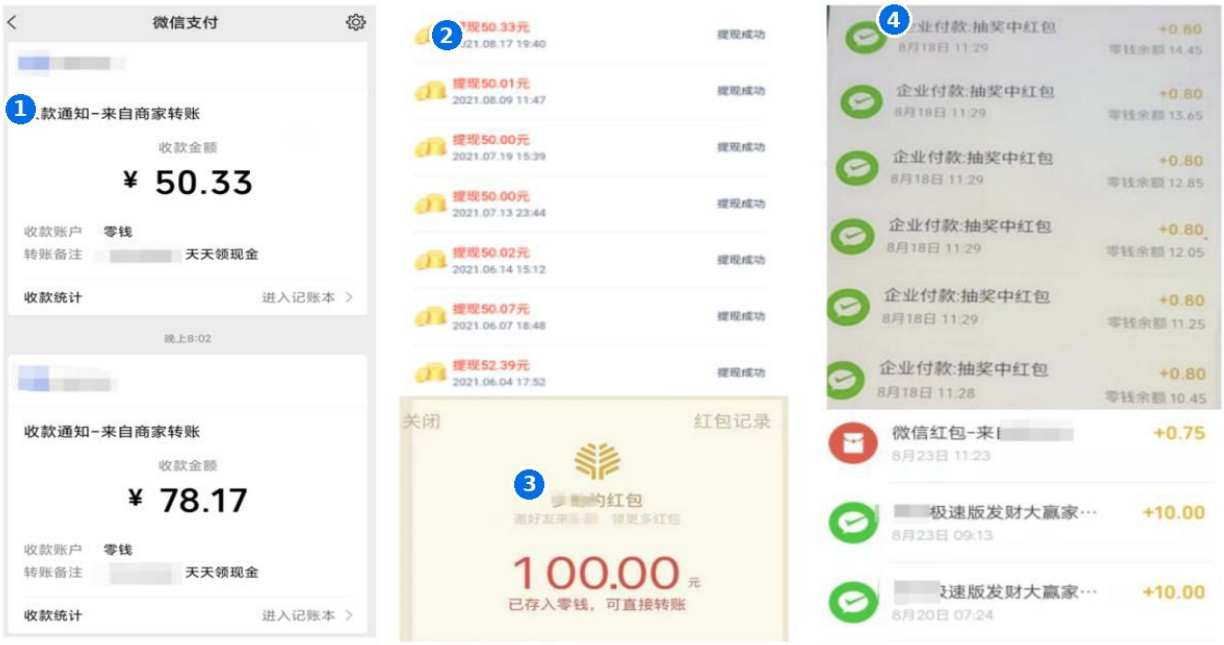
The spread among friends on the super app is the simplest and best marketing fission method for mini programs. In order to stimulate users to repost and share their mini programs more, companies will provide users with various incentives that are attractive enough, and these often become cybercriminal groups' profit methods. The main profit methods are as follows:



How threat actors profit from mini programs: cash red envelopes come first

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

Cash red envelopes: Digital cash red envelopes have been integrated into our lives, and many companies also use cash red envelopes in mini programs to market and acquire customers. Since cash red envelopes can be quickly realized through in-app payment, cash red envelopes have become the most favored way for cybercrime ecosystem to make money, and threat actors also like to use withdrawal records to show off their "achievements":



Threat actors show off cash withdrawals from mini-program campaigns

Source: Threat Hunter original report, page 8. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Payment notices: "Payment received from a merchant transfer" of 50.33 and 78.17 yuan into the wallet balance; transfer note "Daily cash"
2	Withdrawal records: 50.33, 50.01, 50.00, 50.00, 50.02, 50.07 and 52.39 yuan (June–August 2021), all "Withdrawal successful"
3	A red envelope of 100.00 yuan, "deposited to the wallet balance and ready to transfer"
4	Wallet entries: "Business payment: lottery red envelope" of 0.60–0.80 yuan each (18 August), plus 10.00 yuan twice from a lottery mini-game (20 and 23 August)

Although the amount of cash obtained by a single account is often not high, since the attack applet can easily be scaled up, the overall income obtained by cybercriminal groups will be very high.

Lottery: Although the lottery is a probabilistic event, due to cybercriminal groups' advantage in "heads", it is basically guaranteed to make a steady profit; and some lottery prizes themselves are cash red envelopes, and there are even some high-value products, such as flagship smartphones, branded sneakers, etc., which will make cybercrime ecosystem flock to them.

Points: Earn points by completing tasks, and then the points can be exchanged for rewards. Some rewards include cash red envelopes or easily cashable products, such as recharge of phone bills, so they will also attract many cybercrime operators.

Product bargains/coupons: Mainly from many e-commerce platforms on mini programs, use these two methods to market your own products. cybercriminal groups will focus on high-quality or popular products, as well as coupons with high discounts and no-threshold coupons.

Virtual/physical goods: Virtual goods that are commonly used in marketing activities are relatively easy to sell, such as membership cards of major video websites, shopping cards on e-commerce platforms, and offline product redemption coupons. Although physical goods can be sold through platforms such as Xianyu and Zhuanzhuan, the long realization cycle and the cost of sending and receiving goods make cybercrime ecosystem relatively cautious and generally choose daily

necessities (such as paper towels, cooking oil, etc.) and popular Internet celebrity items (such as popular blind boxes, Starbucks cups, etc.).

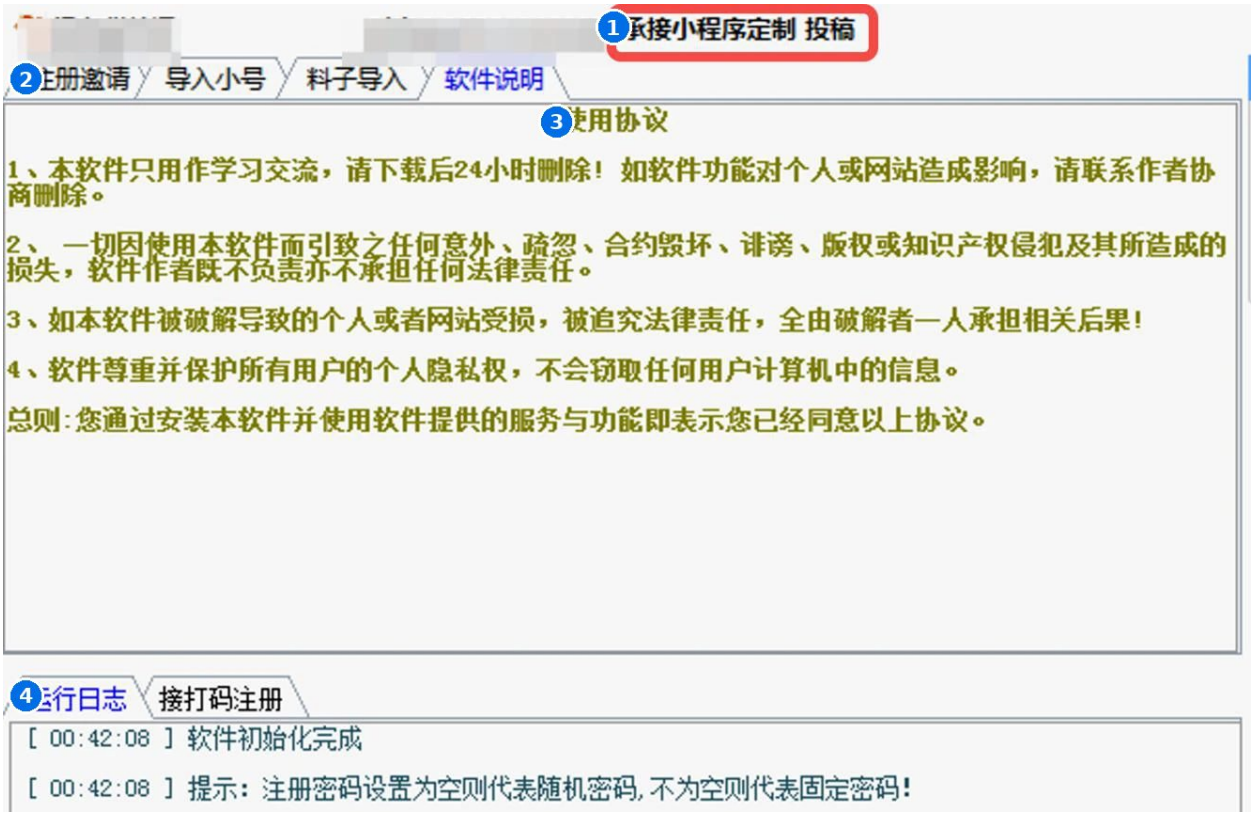
1.5. The cybercrime ecosystem around mini programs has formed a mature industry chain

To judge whether an industrial chain is mature, we can evaluate it from two aspects: 1. Whether there is a stable group of practitioners; 2. Whether a stable supply relationship has been formed. In the cybercrime ecosystem chain surrounding mini programs, account supply and automated tool development are key links, and a relatively stable practitioner population and supply relationship have been formed.

Account supply: The account resources of mini programs were mainly sold through card issuance platforms or Q group advertising in the early days, with little reach.

The quantity and stability cannot be guaranteed; and currently there is a cybercrime ecosystem: the authorized-login platform that specifically provides authorized login for mini programs. On the one hand, account resources are fully guaranteed, and on the other hand, it also better connects upstream and downstream. According to our statistics:

- There are currently more than 10 active authorized-login platforms
- The number of super-app accounts that can be used to log in to mini programs on the head platform exceeds one million
- Most platforms support API docking and can be quickly integrated into automated attack tools. Automated tool development: More and more cybercrime ecosystem tool authors are involved in the development of mini program attack tools. Some tool authors will also advertise on the program interface to undertake the customized development of mini program attack tools:



An attack tool that advertises custom mini-program tools on its interface

Source: Threat Hunter original report, page 10. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Banner (boxed): "Custom mini-program tools made to order"
2	Tabs: "Register invitations", "Import secondary accounts", "Import material" and "Software notes" (selected)
3	Usage agreement: for study and exchange only, delete within 24 hours of download; the author accepts no liability for any loss; if the software is cracked, the cracker alone bears the legal consequences; the software does not steal user data; installing it means you accept these terms
4	Run log: "Software initialized" and "Tip: leave the registration password empty for a random password, or fill it in for a fixed one"

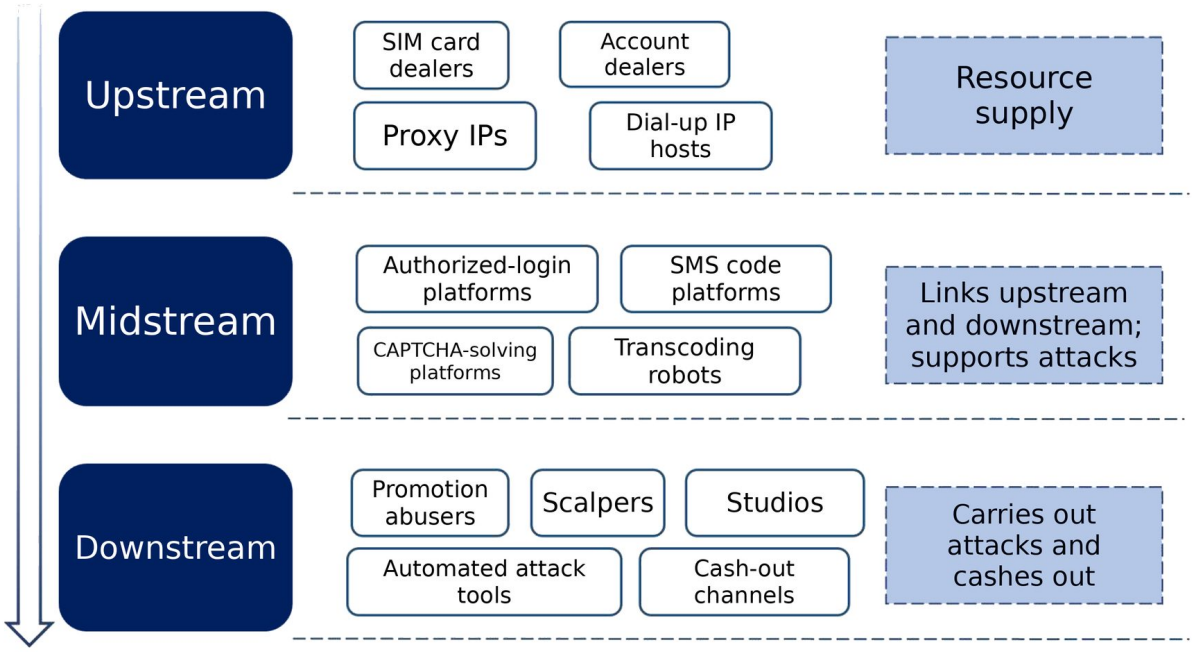
According to our statistics, in the past 1 month:

- More than 90 tool authors have published attack tools targeting mini programs
- The top 10 tool authors have published more than 10 times
- The No. 1 tool author has published 57 times, nearly 2 times per day. In the next chapter, we will further analyze the industry chain and reveal more details.

2. Analysis of mini program cybercrime ecosystem chain

The cybercrime ecosystem chain surrounding mini programs can be roughly divided into upstream, midstream and downstream according to different roles and division of labor.

The upstream supplies resources, the downstream implements attacks and monetizes, and the midstream connects the upstream and downstream and provides assistance for attacks. As shown below:



The mini-program fraud chain: upstream supplies resources, midstream connects and assists, downstream attacks and cashes out

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

Some roles are unique to the mini program cybercrime ecosystem chain, so let’s focus on them.

2.1. Upstream of the industrial chain

- Number merchants

Login to the mini program must be through a super-app account, so the mini program account resource is essentially a super-app account. There are two main types of super-app accounts sold by cybercrime ecosystem:

1. human participant accounts: Most of these accounts come from people who are not financially well-off. When they are in financial distress, they use their personal super-app account to

Rent or sell. Since they are genuine-user accounts, such accounts are basically not restricted by the platform when they enter the cybercrime ecosystem. They are often used by threat actors for some huge profits or illegal activities, such as advertising traffic, online gambling, online fraud, etc. Of course, the selling price of such accounts is also very high, with one account usually costing hundreds.

2. Machine account: This type of account mainly comes from the account farming studios. Nowadays, cybercriminal groups are also advancing with the times, and there are specialized

A platform that provides account maintenance services. The account maintenance studio realizes cloud account maintenance by calling the interface provided by the platform. For example, a certain cloud account maintenance platform provides a very rich account maintenance interface:

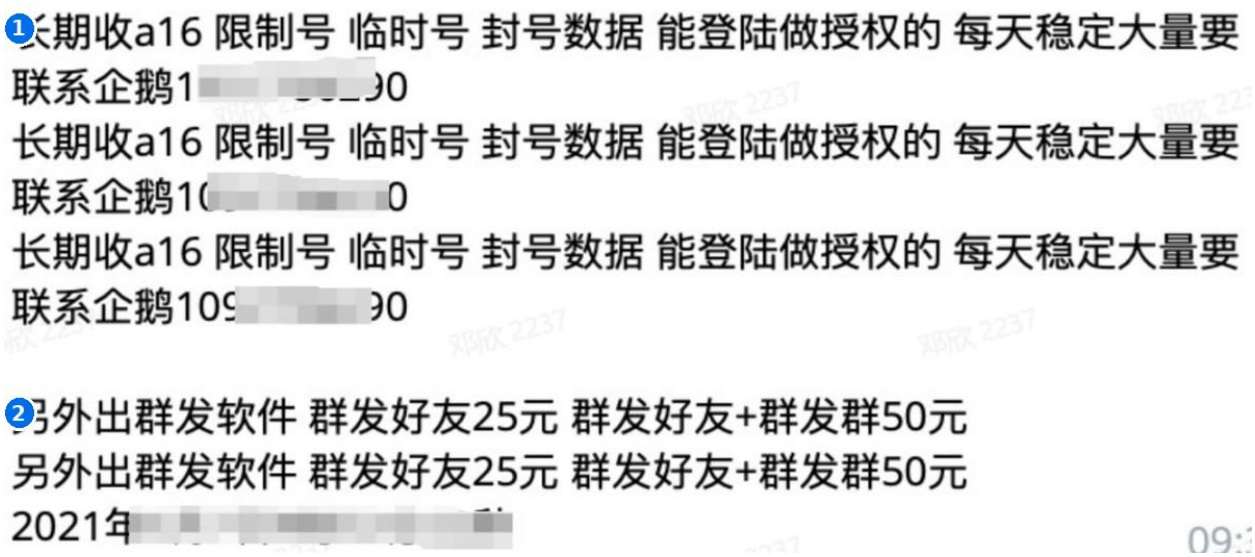
Login	Download message content	Send messages	Friend operations
Get QR code (step 1)	Download file	Send text message	Forward a received image
Get login QR code (step 2)	Download voice	Send image message	Forward a received video
Confirm login	Download voice	Send video message	Add friend
Get personal account details	Download video	Send voice message	Delete friend
Check whether online	Download image	Send link message	Edit friend remark
		Send contact card	Accept friend request
		Send mini program	Accept friend request
		Send file	
		Send animated image	
		Forward a received image	
		Forward a received video	

API functions offered by a cloud account-farming platform

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

The studio only needs to purchase the services of the cloud platform without investing in equipment, and the fraud controls and confrontation are all handled by the cloud platform. Professional matters are left to professional people, and the division of labor is more detailed.

Whether it is a account operated by a real user or a machine account, if it is later restricted by the platform due to illegal activities, it can still be used to log in to the mini program. There are a large number of restricted super-app accounts on the cybercrime ecosystem market, and there are account merchants who specialize in collecting a16 or 62 data, authorizing third parties to log in, including mini programs, official accounts, etc.:



An account dealer buys a16 login data from restricted accounts

Source: Threat Hunter original report, page 12. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	"Buying a16 data long-term: restricted, temporary and banned accounts that can still log in and authorize; large, steady volumes wanted every day. Contact (number blurred)" (posted three times)
2	"Also selling mass-messaging software: messages to friends 25 yuan; friends plus groups 50 yuan" (posted twice)

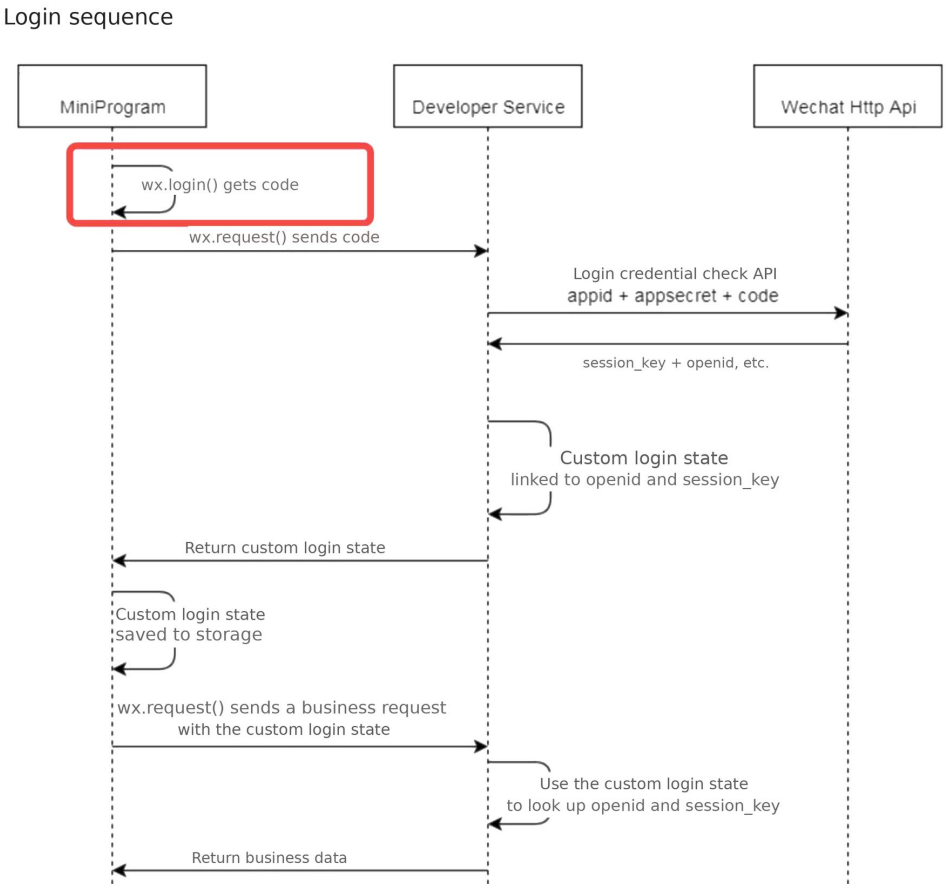
A16 and 62 data are identity credential data generated after logging in to the super app. With a16 or 62 data, you can log in to the super app without account password and verification.

2.2. Midstream of the industrial chain

- authorized-login platform

It is inefficient to directly connect account providers and downstream companies, so a platform connecting account providers and downstream companies emerged: the authorized-login platform.

To understand the authorized-login platform, we must first understand the principle of super-app authorized login. The platform's official developer documentation describes the mini program login process. The flow chart is as follows:



The mini-program login sequence from the official platform documentation

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

To sum up, it can be divided into 2 steps:

1. Call wx.login() to obtain the temporary login credential code and send it back to the developer server;

2. After the developer server gets the code, it initiates a login request to the platform's login service, and the platform's login service returns

Important data such as session_key and openid are sent to the developer server to complete the login and return to the customized login state.

The role of the authorized-login platform lies in step 1. cybercriminal groups can obtain the code through the authorized-login platform without calling wx.login(). On the one hand, attacks against mini programs are completely separated from the operating environment of mini programs. On the other hand, the authorized-login platform reserves a large number of super-app accounts, which can provide a large number of account resources for attacks. Most authorized-login platforms provide API interfaces that can be easily integrated into automated attack tools. The following is the API interface description of one of the platforms:



API documentation of an authorized-login platform

Source: Threat Hunter original report, page 14. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	API address: /prod-api/syste...authorizationUser (partly blurred)
2	Request method: GET
3	API description: "Check status code = 200; on timeout, −1 exits the loop"
4	miniAuthType: the mini-program authorization type. 1: return only the code; 2: return code, encryptedData, iv, nick_name, avatarUrl and signature; 3: bind the mini program to any phone number and return code, encryptedData, iv and mobile. Default: 1

You can see that in addition to the code, the bound phone number, nickname, personalized signature and other information can also be obtained.

There are currently more than 10 active authorized-login platforms. The cumulative number of apps and applets supported by these platforms reaches tens of thousands. Apps and applets that can provide cybercrime ecosystem profit margins are basically on the support list.

- Transcoding robot Transcoding robot is also a unique product of the mini program cybercrime ecosystem: for attackers, it is necessary to specify the beneficiary, such as attack assistance invitation activities, and the initiator of the invitation needs to be specified in the attack parameters. In this case, a transcoding robot is needed.

Take a certain brand of car company's mini program to attract new customers as an example:



How a transcoding robot turns an invitation link into a mini-program code

Source: Threat Hunter original report, page 15. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Step 1: send the invitation link to the transcoding robot (chat group "Transcoding VIP group 2"). The shared card reads "Your friend invites you to try [blurred] cars; tap to unlock car life"
2	Step 2: the robot extracts the mini-program page details, including "points remaining: 82", the page path and the inviter parameters (boxed)
3	Step 3: the robot turns the page details into a mini-program code

1. Log in to the applet with the threat actors income account and send the invitation link to the transcoding robot.

2. The transcoding robot can automatically extract link information, mainly the page and parameters that jump after opening the mini program.

It contains the identity information of the inviter.

3. Some threat actors will also use human-operated fraud platforms (about human-operated fraud platforms, you can read Threat Hunter’s previous post

"Research Report on human-operated fraud cybercrime ecosystem"), inviting human participants to assist in fraud. Therefore, the transcoding robot will also convert the link information into a mini program code to facilitate the in-app code scanning operation.

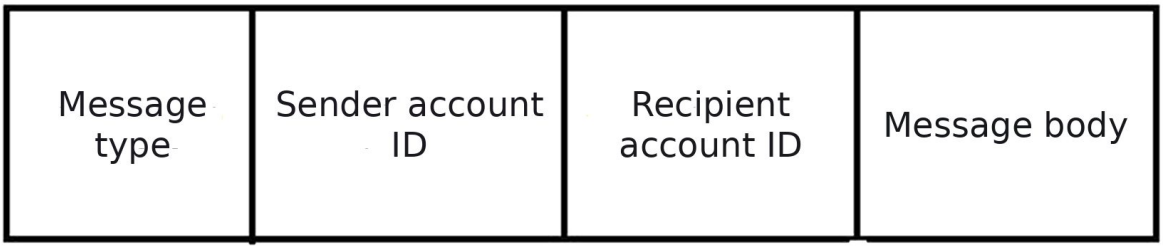
Transcoding robots are generally paid per use, but there are also some free transcoding robots, and some cybercrime ecosystem technology forums even open source the code. Here we briefly introduce the transcoding robot implemented using the super app's PC client. The principle is as follows:

1. Start the PC client and inject the message interception module into the client process;

2. Message interception module hook is the key function that the client uses to receive messages;

3. Determine the type of message received. If the mini program forwards the message, parse and extract the link information.

The text, pictures, emoticons, mini programs and other messages we send are consistent in message format:



Format shared by every message type

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

Different types of messages will have different message bodies. For mini programs, the message body is a text in XML format, in which the tag <weappinfo> contains relevant information, as shown below:

```
<weappinfo>
    <pagepath>
    <![CDATA[packageCommunity/pages/copartner/passiveReferredInfo/passiveReferredInfo.html?shareId=7065
    8&activityType=2&clueName=  1 伙人&shareVin=LGBH52I          6&shareUnionid=oMiuet_9uAxfau7U8N
    FoeTgb2ZuE&_smwt_ks=1624779534820552l9&_smwt_kn=1&_smwt_kr=1624779534820552l9]]></pagepath>
    <username>gh_e574c29a84d2@app</username>
    <appid>wxe3fd49854884240e</appid>
    <version>111</version>
    <type>2</type>
    <weappiconurl>
    <![CDATA[http://wx.qlogo.cn/mmhead/Q3auHgzwzN                                    51r4Ptib7KDg/96]]>
    </weappiconurl>
    <weapppagethumbrawurl>
    <![CDATA[https:/                    /resources    wxmp-site/images/packageCommunity/asst
    es/images/recommend_main_pic.png]]></weapppagethumbrawurl>
    <shareId><![CDATA[1_wxe3fd49                                  5fa6cf27f31ae_1626309630_0]]></shareId>
    <appservicetype>0</appservicetype>
    <secflagforsinglepagemode>0</secflagforsinglepagemode>
    <videopageinfo>
        <thumbwidth>720</thumbwidth>
        <thumbheight>576</thumbheight>
        <appthumburl><![CDATA[(null)]]></appthumburl>
        <fromopensdk>0</fromopensdk>
    </videopageinfo>
</weappinfo>
```

The XML body of a forwarded mini-program message

Source: Threat Hunter original report, page 16. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	The XML body of a mini-program message: <weappinfo> holds the page path and its parameters (including clueName "...partner", shareVin and shareUnionid), plus username, appid, version, type, icon URL, thumbnail URL and shareId

2.3. Downstream of the industrial chain

- Crack mini program

The downstream is the direct initiator of attacks, and for professional cybercrime ecosystem, tools will be developed to implement automated attacks to obtain greater benefits. The first step is to crack the applet and figure out the business logic and core algorithm of the applet.

The cracking steps are as follows:

1. Extract the mini-program package: The mini-program package for the mobile super app is located at:

{{App data directory}}/{{User hash value}}/appbrand/pkg directory, suffix

It is a .wxapkg file; the PC client applet package is located in the directory: {{PC client data directory}}\Applet\{{Mini Program AppID}}\{{Mini Program Version}}, a file named __APP__.wxapkg;

2. Unpack the mini program package: The file structure of the mini program package has been clearly studied and made public. There are also open source projects on the Internet.

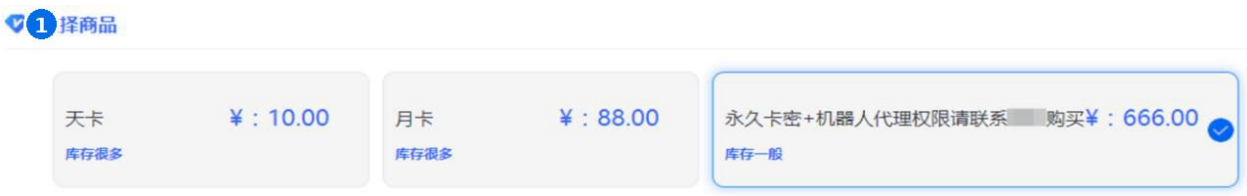
Projects and tools can extract source code files from mini program packages;

2. Analyze the code: Import the source code into the official developer tool to facilitate reading and debugging, and combine it with dynamic packet capture and determination.

Bit and analyze key codes, such as the construction of business interface requests.

- After the development tool completes the cracking of the mini program, the tool developer usually first manually tests to complete the attack process, and then writes the tool code to realize the automated operation. Developers will access the API interfaces of multiple authorized-login platforms in the tool, and will also access the API interfaces of the SMS verification-code receiving service, CAPTCHA-solving service, and agent IP platform. These are all reusable. For different mini programs, tool developers do not need to modify much code, so the cost of developing a new mini program attack tool is not high for them.

After the tool is developed, the developer will sell it to those who carry out the attack through some channels. Some tools are sold publicly, and chat groups are usually used to keep in touch and communicate, including usage tutorials, tool update notifications, download and purchase addresses, etc. The purchase address generally points to a store on a certain card issuance platform. Developers earn revenue by selling card keys, which are priced based on the length of use of the tool:



A tool developer prices license keys by how long the tool can be used

Source: Threat Hunter original report, page 17. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	"Select product": day key 10.00 yuan (plenty in stock); month key 88.00 yuan (plenty in stock); "lifetime key plus robot reseller rights, please contact" (some stock); "Buy: 666.00 yuan"

Some tool developers will develop agents to acquire more users and expand their profits; some tool developers will also launch attacks themselves. In order to reduce risks, they will provide the

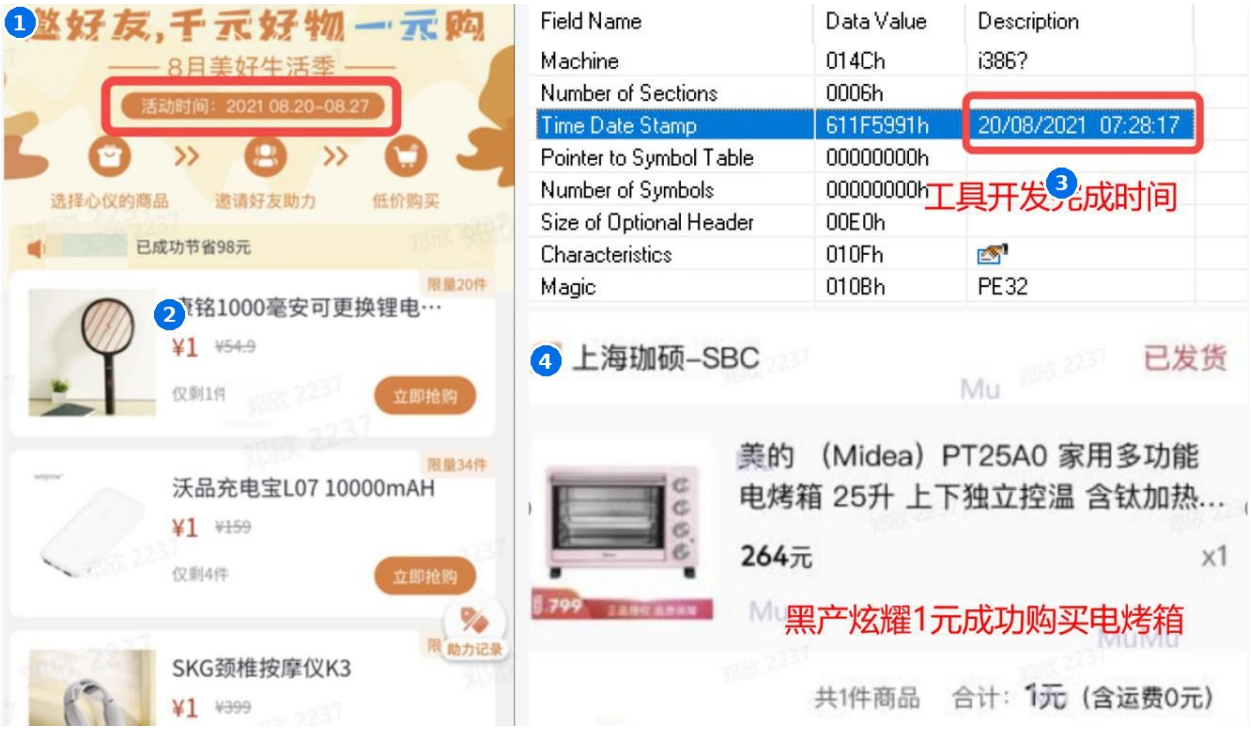
tools for free after a period of time, thereby achieving the effect of "the law does not punish the public".

3. Analysis of mini program attack cases

After understanding the industry chain, we selected several typical cases to give everyone a more intuitive and realistic experience of cybercriminal attacks on mini programs.

3.1. The one-yuan purchase activity of a financial service platform was attacked

From August 20 to August 27, a leading financial service platform's mini program launched the "Invite friends, buy good items worth 1,000 yuan for 1 yuan" activity. You can invite friends to help you bargain, and the price of the product can be reduced to 1 yuan at most. This is attractive enough for the cybercrime ecosystem. At around 7 a.m. on the 20th, that is, more than 7 hours after the event started, a tool author completed the development of an automated attack tool. After the attack was successful, some cybercriminal groups also showed off the profits:



A financial service platform's 1-yuan campaign was attacked within hours

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

Figure guide

1	Campaign: "Invite friends, buy 1,000-yuan goods for 1 yuan", dates 2021.08.20–08.27 (boxed). Steps: choose a product, invite friends to assist, buy at a low price
2	Products such as a bug zapper, a power bank and a neck massager, each for 1 yuan; "Limited", "Only a few left", "Buy now"
3	Tool file header: time stamp 20/08/2021 07:28:17 (boxed); red note: "time the tool was finished"
4	Order: an electric oven worth 264 yuan, "Shipped", total 1 yuan (shipping 0); red note: "A threat actor shows off buying an electric oven for 1 yuan"

Inviting friends to help negotiate prices can quickly achieve user fission through sharing and forwarding of mini programs. Therefore, it is one of the most commonly used marketing methods to acquire customers on mini programs. It is also a very typical mini program attack scenario. Let’s take one of these tools as an example to see how threat actors carry out automated attacks. First, import the list of invitees who need help from the tool interface.

Table:



The attack tool imports the list of inviters to assist

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

Figure guide

1	Tool title: "Bargain V1.0 (no CAPTCHA solving needed)"; "Time remaining: 19,646 days 20 h 42 min 12 s"
2	Tabs: "Registration list" and "Account-farming list"; buttons: "Import data", "Three-part data" and "Ask about the software"
3	Result: "Login succeeded | assist succeeded | 0.95"

Then obtain the assist account code through the authorized-login platform and authorize the login applet:



The tool logs in to the mini program with a code from an authorization platform

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

Figure guide

1	String: "Authorization failed: no authorization obtained"
2	Red note: "login API"
3	Red note: "pass in the code obtained from the authorization platform"
4	Red note: "forged request headers"
5	Strings: "Login succeeded | assisting" and "Login failed | reason:"

After successful login, attack the assistance interface to complete the assistance to the threat actors inviter account:



The tool calls the assist API for the threat actor's inviter account

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

Figure guide

1	Red note: "assist API"
2	Red note: "pass in the inviter ID"
3	Red note: "check the response to see whether the assist succeeded"
4	Strings: "Login succeeded | assist succeeded" and "Login succeeded | assist failed | reason:"

3.2. The cash activities of a certain life service platform were attacked

In order to attract users, a life service platform launched a cash activity. There is an activity cycle every week. Within an activity cycle, an account can earn cash by checking in, inviting friends, placing orders, etc., and you can withdraw cash if you exceed 50. As mentioned earlier, cash activities can be quickly realized through in-app payment, which is the most favored way to make money by cybercrime ecosystem. This activity is no exception:



A life service platform's cash campaign was attacked: withdrawals from a single account

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

Figure guide

1	"My cash": 31.29 yuan; "cash expires in 5 days 02:06:46"; "withdraw once you reach 50 yuan"
2	"Share with friends to get cash once more"; tasks: order to earn 4 yuan, claim to earn 0.1, visit to earn 0.18, claim a coupon to earn 0.02
3	Tabs: assist records, cash records (selected), payout posts; entry "Friend assist +1.18 yuan"
4	"My withdrawal records". Red note: "A threat actor shows off one account's withdrawals": 50.16, 50.33, 50.01, 50.00, 50.00, 50.02, 50.07 and 52.39 yuan (June–August 2021), all successful

Although the cash earned each time is not much, for cybercrime ecosystem, a large number of accounts can be obtained through the authorized-login platform, and batch attacks can be carried out with automated tools. The final overall income will be very considerable.

3.3. The rush buying activity of a certain brand of tea beverage company was attacked

This is a limited-time sale event on the mini program. The promotion is buy 1 get 1 free. You can buy 2 coupons for the price of 1 coupon. Since the coupons for this tea drink are very easy to sell, they were targeted by threat actors. During the event, a large number of promotion-abuse actors transaction information appeared:



Coupon trading posts during a tea-drink brand's buy-one-get-one-free sale

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

Figure guide

1	"@all members: bought yesterday ... 32+29; buying back at 51; ... gift cards from the 13th to 20th bought back at 73% of face value"
2	"Sorry, confirmation is a bit slow. The price for the second round crashed, still buying back at 50; please do not rush me, I am chasing others too. Regulars know I am reliable"
3	"Buying 1,000 sets at 48"
4	"Selling one set for 50"
5	"All settled. Something went wrong today and I got stuck for a while, but everything is handled. Thanks for your support"
6	Each post shows the chat group it came from and a blurred poster

At the same time, automated attack tools have also appeared. Before the activity starts, the time, number and delay of the attack can be set on the tool interface:



An automated snap-up tool lets the attacker set the time, count and delay

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

Figure guide

1	Settings: start time 14:58, number of attempts 250, delay 10
2	Buttons: "Delay at set time", "Strike now", "Test" and "Update software"

When the activity time is up, access to the snap-up purchase interface will be automatically triggered:



When the sale starts, the tool calls the snap-up purchase API

Source: Threat Hunter original report, page 22. Original image retained; numbered translations added by Threat Hunter.

Figure guide

1	Red note: "snap-up purchase API"
2	Request template with [price], [skuid], [productId] and [activityNo] placeholders filled in by the tool

4. Difficulties in attack and defense of mini programs and protection ideas

4.1. Attack and defense difficulties of mini programs

As there are more and more attack cases on mini programs, mini program security has gradually attracted the attention of business parties and the security industry. Compared with Apps and Web applications, Mini Programs bring a new plane of attack and defense. The difficulty is that some existing protection solutions cannot be effectively applied to Mini Programs, resulting in less than ideal protection effects. For example, the following solutions:

- Device fingerprint device information is an important input parameter for business security fraud controls. Whether device fingerprinting can achieve better results depends on whether the collected information can form a unique ID of the device and determine whether the device is risky. out of authority and

Due to security considerations such as privacy, there is not much device information that can be collected by the applet. It can collect device information, such as brand model, screen size, resolution, power, network type, etc., but cannot form a unique and stable device ID, and cannot use this information to determine whether the device is risky.

At the same time, since current cybercriminal attacks on mini programs basically use protocol attacks, cybercriminal groups can arbitrarily forge device information in initiated business requests, which makes device fingerprinting minimally effective in protecting mini programs.

- Security scanning scans the front-end and back-end of the mini program manually or automatically to check whether there are application vulnerabilities such as SQL injection, XSS cross-site scripting, directory traversal, and information leakage. However, the current cybercriminal attacks against mini programs are almost never carried out through application vulnerabilities. cybercriminal groups are an automated attack launched by forging business requests. The machine traffic it generates does not carry any vulnerability characteristics or malicious code, and is no different from normal requests.

Security scanning can detect vulnerabilities in mini programs early and avoid vulnerability attacks; but it does not provide any protection against non-vulnerability attacks.

- Security hardening Security hardening refers to a series of obfuscations and transformations on the front-end code of a mini program. While the execution logic remains unchanged, it reduces its readability and increases the difficulty for attackers to analyze the logic of the front-end code, thereby protecting the security of the mini program. Common transformation methods include: string encryption, variable name obfuscation, inserting junk code, calling equivalent transformations, control flow flattening, etc.

Security hardening can indeed raise the threshold of attack to a certain extent and dissuade novice cybercrime operators, but it still cannot defeat cybercrime operators with strong technical capabilities. Moreover, the code logic of the main body of the mini program will basically not change significantly, so the cracking is a one-time operation. As long as the benefits are large enough, the time cost required for cracking is acceptable for cybercrime ecosystem.

In addition, security hardening will inevitably bring about a certain degree of performance loss and stability degradation, and is inconvenient for debugging, so it is not widely used at present. We randomly selected 30 mini programs as analysis targets. After decompiling these mini programs, we found that none of the mini programs had obfuscated and reinforced the code. The situation is not optimistic.

- Interface protection performs signature verification on access to important business interfaces, which is one of the effective means to resist machine traffic. The most common method is to carry a signature (or token) in the interface request parameter or request header. The signature is generated by an algorithm with a certain strength on the front end of the mini program. The back end of the mini program verifies the legitimacy of the signature based on the corresponding algorithm. If the verification fails, it refuses to respond to this request. For the protocol attacks that mini programs mainly face, it can indeed increase the attack threshold. But the problem lies in the asymmetry between offense and defense.

Since the mini program code cannot be updated in real time, once the signature algorithm is cracked, it is necessary to wait until a new version of the mini program is released before the new signature algorithm can be upgraded. Releasing a new version requires a lot of time to comply with the product plan and undergo complete testing, which often leaves enough attack time for cybercrime ecosystem and greatly reduces the protective effect.

Since the protection effects of these existing protection solutions are relatively limited, we need to consider the characteristics of the mini program itself and combine cybercriminal groups attack intelligence and case analysis to tailor security protection suitable for mini programs.

4.2. Ideas for protecting mini programs

- Pay attention to the value of intelligence

"How can you know how to defend against an unknown attack?" Regardless of the product form, intelligence is very important for security offense and defense. Through intelligence, you can immediately sense whether there is an attack on one's own applet and the scale of the attack, and extract the technology and attack logic used by cybercrime ecosystem from the intelligence to carry out targeted countermeasures.

Here is a practical case: last year, a travel company used a mini program to attract users through a game and gave high cash rewards to those who passed the game. Under normal circumstances, players cannot clear the level within the specified time and need to rely on inviting friends to extend the game time. However, analysis of attack tools captured from the Threat Hunter business intelligence platform revealed that threat actors only need to forge interface requests for successful clearance, and can skip game levels and directly receive cash rewards. Based on this piece of information, the business side quickly made repairs to avoid further losses.

- Design reasonable rules. Reasonable rules need to be sufficiently attractive to normal users to ensure normal business operations; on the other hand, they need to increase the cost of cybercriminal attacks or reduce their benefits. Here are some suggestions on rule design for your reference.

1 cash red envelope:

It is not recommended to withdraw money instantly to allow time for review;

2 coupons:

If there are some low-value and easy-to-cash products on the platform (such as 10 yuan to recharge phone bills), no-threshold coupons are not recommended;

3 draws:

For some accounts that may have problems (for example, the IP address comes from the IDC computer room, lack of reporting of hidden activities, etc.), reduce the probability of winning.

4 Assistance to invite/bargain:

This is the most distinctive marketing method of mini programs. Since it is often necessary to invite multiple people, cybercriminal groups will use proxy IPs to avoid the problem of a single IP address when attacking. However, whether it is base station IP or ADSL dial-up IP, there are situations where good people and bad people mix it, resulting in a certain proportion of false alarms. The risk IP will be judged only after the number of people who have hit the risk IP can be large.

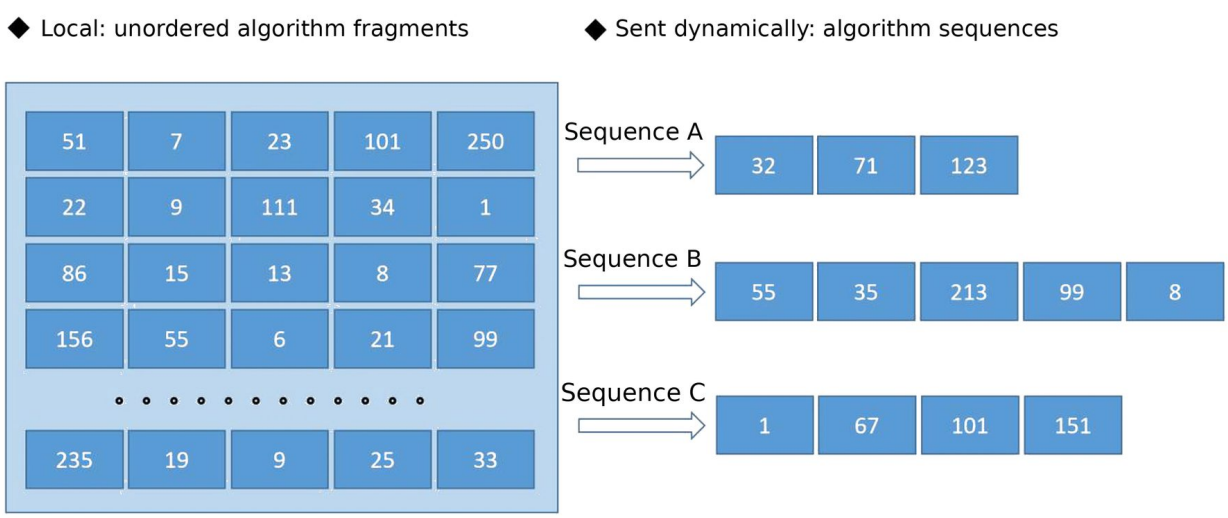
Significantly reduces the false alarm rate.

For example, when assistance requires inviting 5 people, and only 1 person hits the risky IP, the false positive rate is 1%; if 2 people hit the risky IP at the same time, the false positive rate is reduced to 0.01%, and if 5 people hit the risky IP at the same time, the false positive rate is negligible. The threshold for the number of people can be set based on the actual situation.

- Dynamic protection based on mini programs The idea of dynamic protection has been widely used in Apps and Web applications. The core idea is: the attack surface that is more fierce against cybercriminal groups attack and defense, such as the signature algorithm of interface protection, the code is not fixed, but changes dynamically. This makes it difficult for threat actors to find attack anchors and cannot carry out stable attacks.

For mini programs, the difficulty of this solution is that the code of the mini program can only be updated when a new version of the mini program is released, and cannot be dynamically distributed. In theory, only fixed code can be executed. However, we can change our thinking and take the signature algorithm as an example:

An algorithm = several algorithm fragments + fixed execution sequence. We place the algorithm fragments of all signature algorithms in the code file on the front end of the mini program out of order, and then dynamically issue the execution sequence on the back end, as shown below:



Dynamic signing: the server sends one of many execution sequences for the algorithm fragments stored in the mini program

Source: Threat Hunter original report, page 26. Original figure with Chinese text replaced by English.

If there are 100 sets of algorithms, they correspond to 100 execution sequences, and one execution sequence is randomly issued each time to achieve the effect of dynamic signature. However, since all algorithm fragments are exposed locally, even if scrambled and obfuscated encryption is performed, it is difficult to guarantee that it will not be cracked over time. Therefore, it is still necessary to maintain an offensive and defensive confrontation with the cybercrime ecosystem. With the help of intelligence, we can effectively detect whether cybercriminal groups have bypassed protection, so that we can upgrade the algorithm in a targeted manner.

This is also our current main mini program protection solution.

- Written at the end, there is no technical solution that can solve certain types of security problems once and for all. The same is true for mini program security. More people need to participate, brainstorm, strengthen communication and cooperation, and jointly build security. We publish this report in the hope that it will spark more thinking and discussion in the industry and safeguard the healthy development of the mini program ecosystem.

About Threat Hunter

Threat Hunter takes cybercrime ecosystem intelligence capability building and attack and defense technology as its core to provide enterprises with business anti-fraud and API data security solutions. Through the business risk monitoring system, risk intelligence data capabilities and rich offensive and defensive experience of threat actors, it helps enterprises solve business fraud problems such as account security, marketing anti-fraud, traffic fraud, API security, etc., improves defensive effectiveness for enterprise fraud controls, and ensures the healthy development of the enterprise's online business.

Currently, it serves more than 300 enterprise customers across the internet, financial services, securities, and consumer services sectors.