THREAT HUNTER RESEARCH

H1 2018 Cybercrime Tools Report

An early study of the industrialization of cybercrime tools and the shift from simple automation toward more adaptive attacks.

Original publication: 2018-07-31
Research team: Threat Hunter Research Team
Source report: 33 pages

Original report text

This text version is reconstructed based on the 33-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.

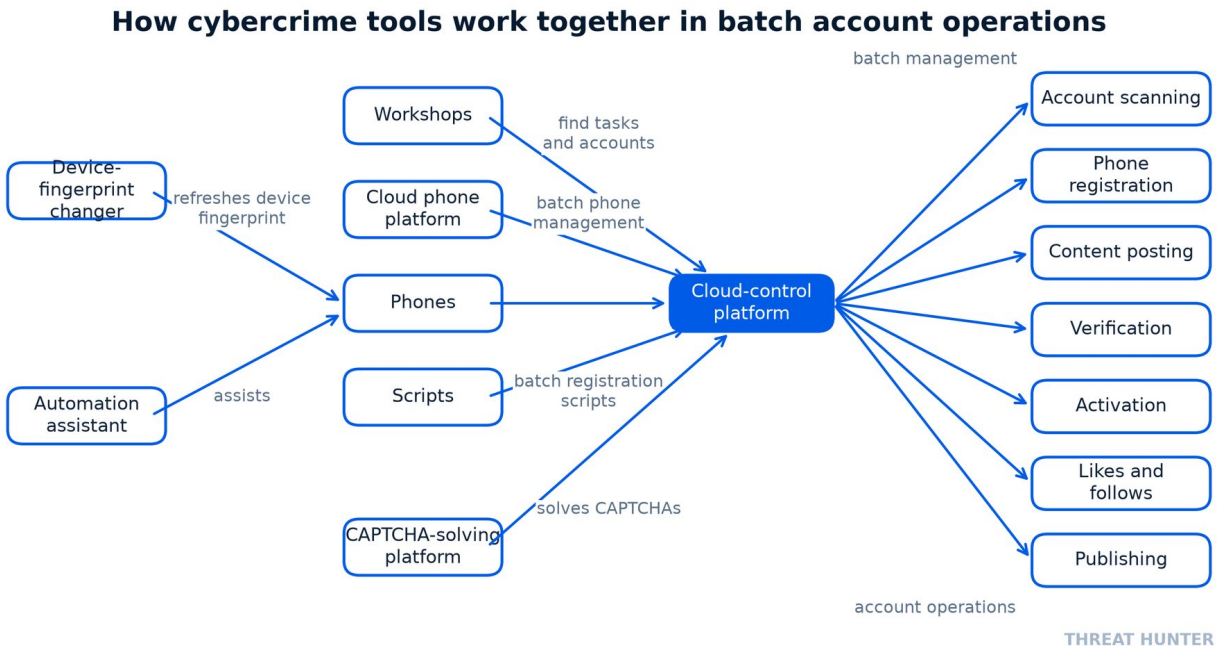
Copyright Statement The copyright of this report belongs to Threat Hunter and is protected by law. No unauthorized reproduction, excerpting or other use of the text or opinions in this report is allowed without permission. If you need to reproduce, please contact Threat Hunter. Anyone who violates the above statement will be held accountable for relevant legal liability.

Contents Preface 1. Characteristic analysis of cybercrime ecosystem tool software 1.1 Deep integration with the industrial chain 1.2 Extremely strong ability to quickly iterate versions 1.3 Obvious trend of profit-seeking 1.4 Wandering in the gray area on the edge of the law 1.5 The phenomenon of gangsters eating gangsters is very common 2. Continuously evolving methods and means 2.1 From simulation scripts to multiple development languages 2.2 From PC to multi-terminal support 2.3 From terminal to cloud 2.4 From mechanical execution to machine learning 3. the cybercrime ecosystem tools active in business security 3.1 Account tool software 3.2 Tool software for traffic manipulation orders and volume 3.3 Tool software for promotion abuse 3.4 Tool software for content crawling 3.5 Tool software for specific functions 4. Analysis of typical cybercrime ecosystem tool software

4.1. Mobile registration bot 3.0 for a video community 4.2. Red-envelope grabbing tool for a social app 4.3. Full-time VIP posting software for a classifieds site 5. Conclusion

Foreword The Wannacry ransomware outbreak in May 2017 had a serious impact, bringing the NSA arsenal into the public eye; in the invisible battlefield of network security, and in another corner of the battlefield - the field of Internet business security, cybercrime operators also have a powerful arsenal in their hands: a variety of tools and software, and they are not well known to people. If phone numbers, accounts, IPs, devices, etc. are ammunition for threat actors, then tool software is the weapon that maximizes the power of these ammunition. The analysis and research of tool software is an important part of the research on threat actors.

1. Characteristic analysis of cybercrime ecosystem tool software We have systematically sorted out and analyzed the cybercrime ecosystem tool software captured in the past six months, and found that the current cybercrime ecosystem tool software has the following obvious characteristics. An in-depth understanding of these characteristics will help us have a more accurate control and judgment on the development of the cybercrime ecosystem.



How cybercrime tools work together: device changers, automation scripts, cloud control and CAPTCHA-solving services feed batch account operations

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

1.1 Deep integration with the industrial chain

With the development and maturity of the cybercrime ecosystem, today's tool software has been deeply integrated into the entire industry chain and has become an irreplaceable part of it. Taking the account registration scenario as an example, in addition to mastering resources such as CAPTCHA-solving services, CAPTCHA-solving services, and dynamic IPs, the cybercrime ecosystem also integrates various tools and software such as machine modification tools, simulated click tools, batch number scanning tools, and agent software tools to achieve a highly automated and highly collaborative work process, as shown below:

1.2 Extremely strong version rapid iteration capability

Compared with normal software, cybercrime ecosystem tool software has faster version update iteration speed. One for

Take the registration-bot software aimed at a major e-commerce platform as an example. From January 2018 to April 2018, we monitored a total of 20 version updates of the software, and frequently updated 2 versions a day, as shown below: Discovery time Software version number January 5, 2018 [Registration client] registration v18.0105.rar January 9, 2018 [Registration client] registration v18.0109.rar January 18, 2018 [Registration client] registration v18.0118.rar January 19, 2018 [Registration client] registration v18.0119.rar January 21, 2018 [Registration client] registration v18.0121.rar January 30, 2018 [Registration client] registration v18.0130.rar February 26, 2018 [Registration client] registration v18.0226.rar March 19, 2018 [Registration client] registration v18.0319.2.rar March 21, 2018 [Registration client] registration v18.0321.rar March 22, 2018 [Registration client] registration v18.0322.rar April 7, 2018 [Registration client] registration v18.0407.rar April 11, 2018 [Registration client] registration v18.04011.rar April 11, 2018 [Registration client] registration v18.04011.2.rar April 15, 2018 [Registration client]

registration v18.04015.rar April 18, 2018 [Registration client] registration v18.0418.rar April 20, 2018 [Registration client] registration v18.0420.rar April 25, 2018 [Registration client] registration v18.0425.rar April 25, 2018 [Registration client] registration v18.0425.2.rar April 26, 2018 [Registration client] registration v18.0426.rar April 27, 2018 [Registration client] registration v18.0427.rar In addition to adding new features and fixing bugs, frequent version updates are a manifestation of the intensified offensive and defensive confrontation between cybercrime operators and business security teams. A typical scenario: After a tool software for company

1.3 Obvious profit-seeking trend

If the hacker tool software in the early years was more or less ostentatious, the current the cybercrime ecosystem tools have become very "pragmatic" and completely driven by profit. In recent years, the Internet has developed rapidly, especially the short video industry, self-media industry and e-commerce industry. A number of Internet companies have boomed in business; and the cybercrime operators who are parasitic on the business of these companies have a very keen sense of "business". Whenever the business is developing

Some weak points have emerged, and tools and software that use this to gain profits will soon appear, among which the promotion abuse tools for marketing activities are the most typical. Meituan launched a football betting activity on the eve of the 2018 World Cup in Russia:

Soon after the event was launched, more than 50 tools and software for the event appeared on the Internet. Among the tools and software related to Meituan’s business, betting software jumped directly to the first place, as shown below:



Promotion-abuse tools appeared within days of a major sports-betting promotion; the original screenshots show the event pages they targeted

Source: Threat Hunter original report, page 8. Original screenshot retained.

1.4 Wandering in the gray area on the edge of the law

Since the promulgation and strict implementation of the "Cybersecurity Law of the People's Republic of China", two obvious changes have taken place among threat actors: one is that more and more people use anonymous communication and anonymous transactions to hide themselves; the other is the tools of threat actors that clearly trigger the law, such as account-stealing Trojans, remote control Trojans, game plug-ins, etc., and fewer and fewer people are doing it. Although there are some people who take risks out of desperation, more people will still weigh the risks and benefits to maximize the benefits and avoid the disadvantages. Take the e-commerce industry as an example. Although some people still use some Trojan-type tools and software to steal and defraud funds, more active are some auxiliary tools and software, such as merchant auxiliary tools, which provide data collection and analysis, store traffic and other functions. Some software also places a disclaimer in a prominent position on the interface (although it may not be useful), as shown below:

Of course, as the law continues to improve and improve, what is currently considered a "grey" area on the edge of the law may no longer be a "safe" area one day in the future, which will inevitably lead to the collective migration of practitioners and related tools and software again.



A tool operating in the grey area: batch account management software with account details masked in red

Source: Threat Hunter original report, page 9. Original screenshot retained.

1.5 The phenomenon of black people eating black people is very common

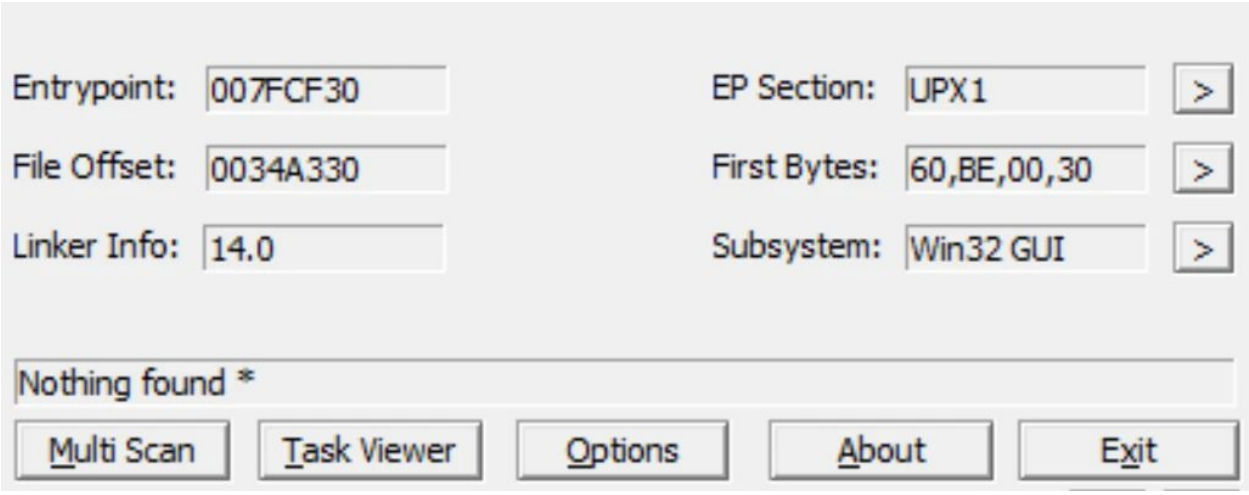
If cybercriminal groups are also a river and lake, not all practitioners will abide by the rules of the river and lake, and the phenomenon of gangsters taking advantage of others is very common. This is also very obvious in the tool software. A large part of the cybercrime ecosystem tools and software spread on the Internet have various problems. For "newbies" who have just entered this world, they may become someone else's meal if they are not careful. According to our analysis, the problematic software tools mainly fall into the following categories: 1. Pretending to be someone else's: This type of tool software does not have the functions it claims to have at all, but will secretly do other things behind the scenarios. The most typical one is a rogue promotion software (note: after running, various "family buckets" will be downloaded and installed in the background), which are widely spread on the Internet with names such as "stimulating battlefield auxiliary plug-ins", "traffic treasure to increase the volume", "grabbing red envelope artifact", etc., with more than 1,000 downloads per day; 2. Buy one, get one free: To put it simply, it is secondary packaging. Some people with ulterior motives package normal software tools and virus Trojans together, and then spread them on the Internet. Since the cybercrime ecosystem tools are often killed and reported as viruses, even if there is a virus, the user of the tool will choose to let it go. People who frequently use the cybercrime ecosystem tools and software often have various viruses on their devices; 3. Please be careful: Before using some cybercriminal groups tools, you need to log in first (for example, tools aimed at one internet group's services must first log in to its messaging apps, and tools aimed at another group's services must first log in to its shopping platform), because in some cases it is necessary to obtain the login status before proceeding to the next operation. However, the entered account number and password are not only used for business login, but also sent to some tool software producers with ulterior motives; 4. Exaggeration: This type generally appears in paid tool software. Buyers spend a lot of money on so-called powerful tools, such as "100% modification of machine code", "VIP member crack", "fully automatic flash sale", etc., but after using them, they find that the actual effect is poor or even ineffective. When buyers of tools encounter this situation, they will definitely have no way to complain and can only grit their teeth and swallow it. We therefore advise those who plan to enter this industry that threat actors are risky and should be cautious when entering the industry.

2. Continuously evolving methods and means According to statistics from the Threat HunterTH-Karma business intelligence monitoring platform, more than 1,000 new cybercrime ecosystem tool softwares are created on the Internet every day, including software updates. These tool software are constantly developing and evolving with the development of Internet technology and IT technology.

2.1 From simulation scripts to multiple development languages

In the early days of cybercrime ecosystem tool software, most attacks were implemented by simulating manual operations. For example, customized scripts were written based on key wizards, desert plug-ins, etc., and operations such as registration, login, and gold coins could be completed through simulated clicks. This method is simple and has a low learning threshold, but the usage scenarios are limited and the efficiency is low. Later, cybercrime ecosystem tool software based on high-level languages □□□□such as VB/C/C++ also appeared. This type of tool software is no longer based on simulating manual operations, but is more based on cracking and replaying network protocols, directly attacking business interfaces, so that more attacks can be launched per unit time and profits can be maximized. However, this type of programming language is more difficult to develop and requires developers to have better programming skills. Today's cybercrime ecosystem tool software is mostly written in Yi Language, C#, Python, Lua and other languages. These languages □□have relatively complete functional modules and frameworks, and many complex functions can be completed with a simple call. They have the advantages of being quick to get started and having a short development cycle. Especially Yi Language and C#, more than 50% of the PC-side cybercrime ecosystem tool software we captured in the past few months were written in these two languages. In addition, in order to protect their core code logic from being discovered by them, many tool software currently use some packers to pack themselves. The picture below is a tool software written based on C# to crack the download speed limit of a popular cloud drive, with a UPX shell added:

Compared with strong shells such as VMProtect and DNGuardHVM, the UPX shell is easier to remove; after removing the shell, you can find



Packer detection on a cybercrime tool: the sample is protected only by the UPX packer, which is easy to remove

Source: Threat Hunter original report, page 11. Original screenshot retained.

Out of its core code logic, the following figure is a code fragment that splices the cloud drive's download link: value: function(e) { var t = this.getPrefixLength(); for (var n in e) this.fileDownloadInfo.push({ name: e[n].path.substr(t), link: location.protocol + "//pcs.[cloud-drive domain]/rest/2.0/pcs/file?method=download&app_id=250528&path=" + encodeURIComponent(e[n].path), md5: e[n].md5 }); return Promise.resolve() }

Cloud-drive download link built by the tool

```
value: function(e) {
    var t = this.getPrefixLength();
    for (var n in e) this.fileDownloadInfo.push({
        name: e[n].path.substr(t),
        link: location.protocol +
            "//pcs.[cloud-drive domain]/rest/2.0/pcs/file?method=download&app_id=2505…
            &path=" + encodeURIComponent(e[n].path),
        md5: e[n].md5
    });
```

THREAT HUNTER

Core code of the tool: it builds a cloud-drive download link from each file path

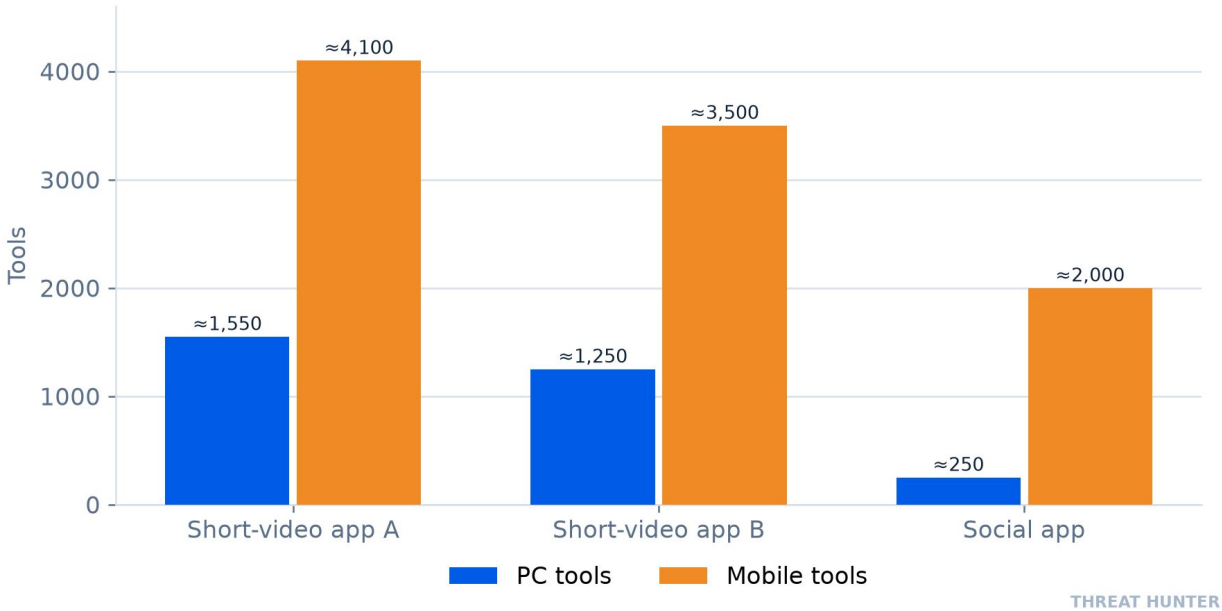
Source: Threat Hunter original report, page 11. Redrawn in English from the original figure.

2.2 From PC terminal to multi-terminal support

With the rapid development of mobile Internet in recent years, a new service experience and lifestyle have been created; Internet products, services and users have also migrated from PC to mobile. For cybercrime operators, the tool software they use has also evolved from PC to mobile. Judging from the current hottest short video industry, we have captured a large number of cybercrime-related tool software in the past few months, and the number of mobile terminals has far exceeded that of PC terminals, as shown below:

Compared with PC tool software, mobile tool software can achieve lower confrontation costs through plug-ins. After our analysis, among the cybercrime ecosystem tools captured in the short video industry, there are a large number of them based on the Android version of a popular automation app.

Number of PC and mobile cybercrime tools by targeted app



THREAT HUNTER

Cybercrime tools captured for three apps in the monitoring sample: mobile tools outnumber PC tools for every app

Source: Threat Hunter original report, page 12. Redrawn in English; values read from the original chart and approximate.

Cybercrime tools written for Android cover the core business scenarios of cybercrime ecosystem such as registration, traffic manipulation, and traffic diversion, as shown below:

Function	Package name (social app name removed)
Registration bot	Batch registration 2018-05-01_015811.apk
Registration bot	Batch registration 2018-05-01_134610.apk
Registration bot	Batch registration 2018-05-01_170054.apk
Registration bot	Batch registration 2018-05-09_103551.apk
Registration bot	Batch registration 2018-05-10_130412.apk
Registration bot	Batch registration 2018-05-16_155650.apk
Traffic manipulation	Comments 1.0 2018-04-09_024220.apk
Traffic manipulation	Comments 1.2 2018-04-09_195258.apk
Traffic manipulation	Comments 1.5 2018-04-14_193518.apk
Traffic diversion	Group diversion 2018-05-17_163550.apk
Traffic diversion	Group diversion 2018-05-17_172801.apk
Traffic manipulation	Live-room boosting 1.0 2018-03-18_160047.apk
Traffic manipulation	Live-room boosting 1.3 2018-03-18_200441.apk
Traffic manipulation	Live-room boosting 1.3 2018-03-18_200441.apk (1).1
Traffic diversion	Diversion 2018-01-27_195531.apk
Traffic diversion	Diversion 2018-05-11_002728.apk
Traffic diversion	Diversion 2018-05-11_111238.apk
Traffic diversion	Diversion 2018-05-13_101822.apk
Traffic diversion	Diversion 3.0 2018-03-15_234312.apk
Traffic diversion	Diversion 3.9 2018-04-02_174144.apk
Traffic diversion	Diversion 4.1 2018-04-13_142437.apk
Traffic diversion	Diversion 4.2 2018-05-15_150425.apk
Traffic diversion	Diversion 4.2 2018-05-15_150425 (copy).apk
Traffic diversion	Diversion 4.3 2018-05-16_060243.apk
Traffic diversion	Diversion v4.0 2018-04-06_225322.apk
Traffic diversion	Diversion -Feiyuan-4.22.apk
Traffic diversion	Diversion script 2018-03-18_172620.apk
Traffic diversion	Diversion script 4.10 2018-04-10_223129.apk
Traffic diversion	Diversion script 18 April.apk
Traffic diversion	Diversion script official release.apk
Traffic diversion	Diversion software 2018-03-14_223954.apk

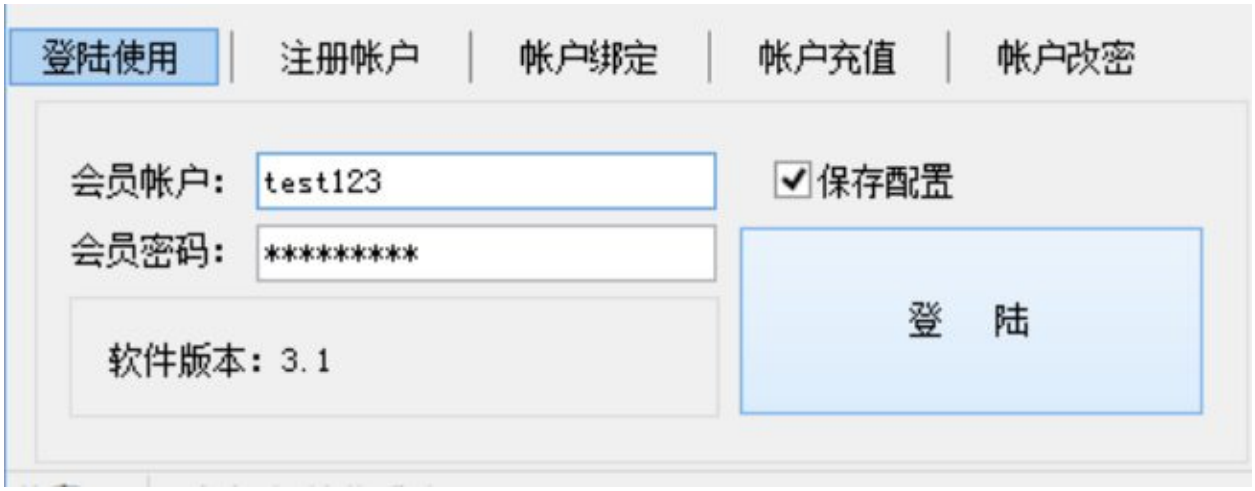
Android tools for one social app cover registration, traffic manipulation and traffic diversion

Source: Threat Hunter original report, page 13. Table re-typeset in English from the original; platform names replaced with neutral wording.

2.3 Development from terminal to cloud

If the development of cybercrime ecosystem tool software from PC to mobile is the current trend, then moving from terminal to cloud is the future trend. Some tool software has already reflected this characteristic. Take the software we analyzed to increase video playback volume as an example. Starting from July this year, the terminal tool software only retains basic functions such as login, registration, and recharge. After logging in, you can publish tasks, but the core logic of increasing video playback volume has been placed in the cloud:

There are two main reasons that promote the development of tool software from terminals to clouds: 1. The development of cybercrime ecosystem technology, especially the development of group control/cloud control systems and other technologies, has enabled some cybercrime operators to have a large number of accounts and equipment resources in their hands, as shown in the figure below:



Cloud-control client: users log in to a member account and the work runs on the operator's cloud

Source: Threat Hunter original report, page 14. Original screenshot retained.

Figure 2 For these people, they no longer need to develop specialized tool software for use on downstream terminal devices. The downstream only needs to submit task requirements through web pages or other methods, and all actions can be completed on the large number of cloud devices they control; 2. Terminal cybercrime ecosystem tool software, even if it is only spread in a small circle, can be easily obtained by the outside world, and then the core logic of the tool can be obtained through reverse analysis and other methods, so that it is blocked by the business side or imitated by others; cloudization hides the core logic of the tool to the back end, which is a black box for the outside world, making it much more difficult to block or imitate.



Figure 2: a cloud-control platform managing large numbers of phones from one console

Source: Threat Hunter original report, page 14. Original screenshot retained.

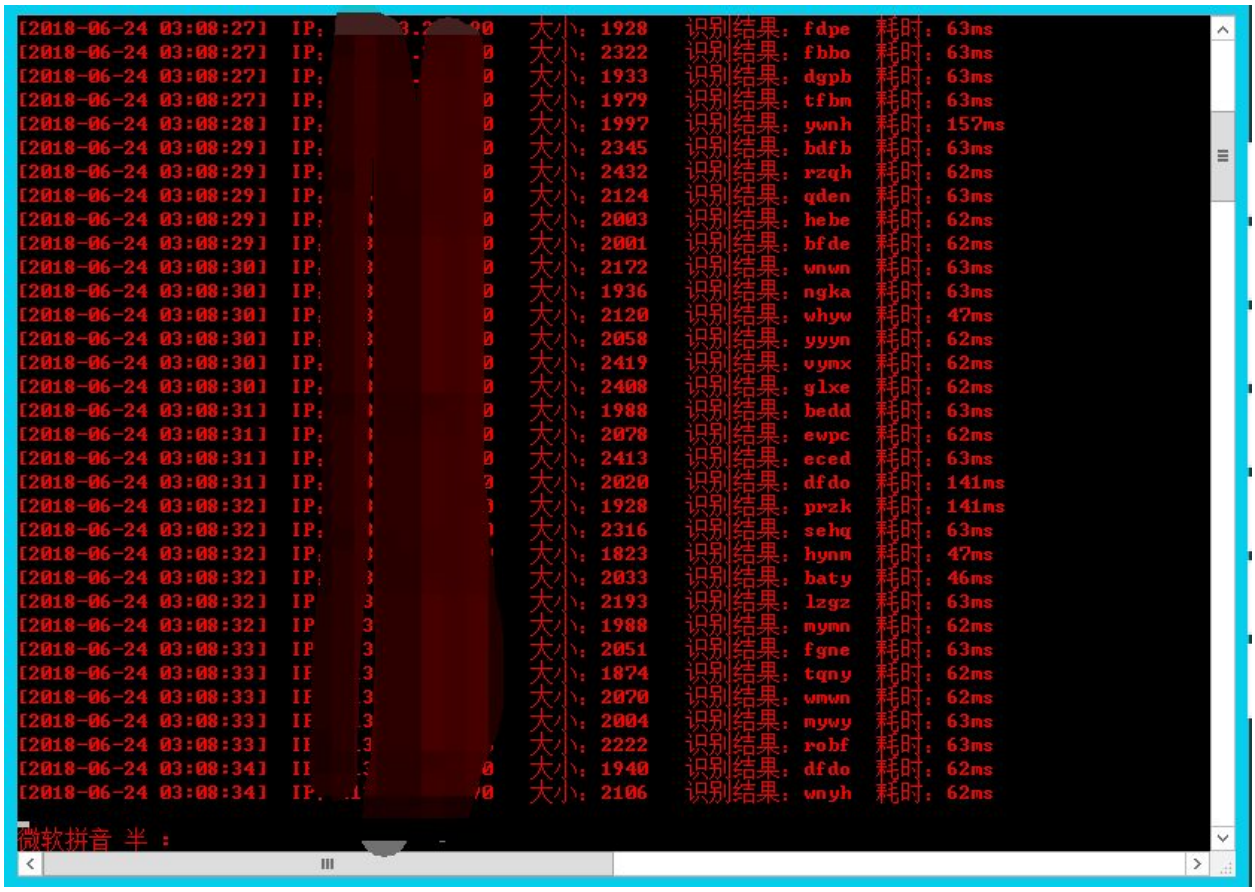
2.4 From mechanical execution to machine learning

In early tool software, the core execution logic was mostly Hardcoded in the program code, or specified by writing task scripts. Although simple to write, they all mechanically execute fixed logic. Not only do they lack scalability and adaptive capabilities, for example, different scripts need to be written for different screen resolutions, but they are also easier to detect and intercept. With the continuous development of IT technology, especially in recent years, machine learning and deep learning have made great progress in areas such as image recognition, and the cybercrime ecosystem tool software has also completed its own technical upgrade. Take verification codes as an example. companies use verification codes to identify people and machines. They have evolved from simple letters/digits to the popular slider verification codes, and even various combinations of verification codes. On the other hand, cybercrime operators now have a complete verification code recognition system based on deep learning. Both the response speed of obtaining verification codes and the recognition accuracy are much higher than traditional CAPTCHA-solving services (note: traditional CAPTCHA-solving services mainly rely on manual input or a verification code recognition library generated for a certain website). As shown in Figures 3.1 and 3.2:



A CAPTCHA-solving platform advertises machine-learning recognition, accuracy and anti-detection features

Source: Threat Hunter original report, page 15. Original screenshot retained.



A verification-code solving server at work: request logs scroll as codes are recognized automatically

Source: Threat Hunter original report, page 16. Original screenshot retained.

Figure 3.2 Another typical example is face authentication. Professional facial authentication software can quickly generate a 3D face model through a simple selfie, and quickly simulate a face to perform simple authentication actions, thereby bypassing face recognition in the registration or login process.

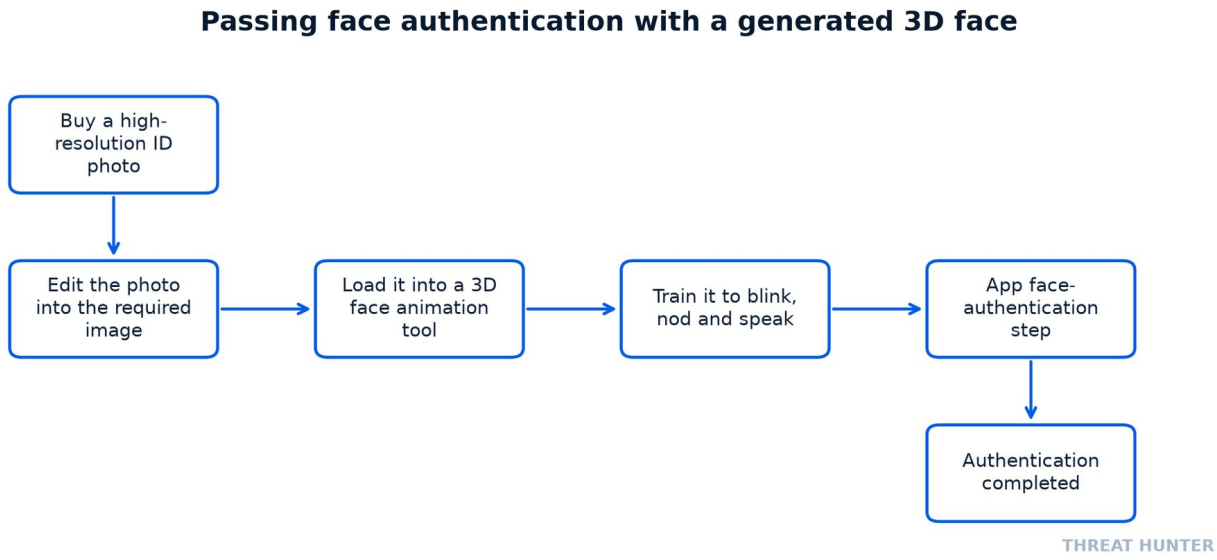


Figure 3.2: how fraudsters pass face authentication with a generated 3D face model

Source: Threat Hunter original report, page 16. Redrawn in English from the original figure.

3. the cybercrime ecosystem Tools Active in Business Security Based on the cybercrime ecosystem tool software intelligence analysis we captured, currently active tool software can be roughly divided into five categories based on business functions: account type, volume traffic manipulation type, promotion abuse type, content crawling type and specific function type. The proportion of the number of tools of each type is shown in the figure below:

Figure 3-1 Proportion of tool function types In business security confrontation, order traffic manipulation is the most commonly used attack tool in the cybercrime ecosystem, and it is also the most active type of tool, such as increasing article reading, increasing video playback, increasing the number of fans, and increasing the number of orders, etc. This type of attack is concentrated in the self-media industry, e-commerce industry, and video industry; in addition, account type, promotion abuse, and content crawling tools are also active in cybercriminal. Underground is fighting against the business security of companies; specific function tools mainly include functional tool software such as simulators, multi-open, computer modification, and dial-up.

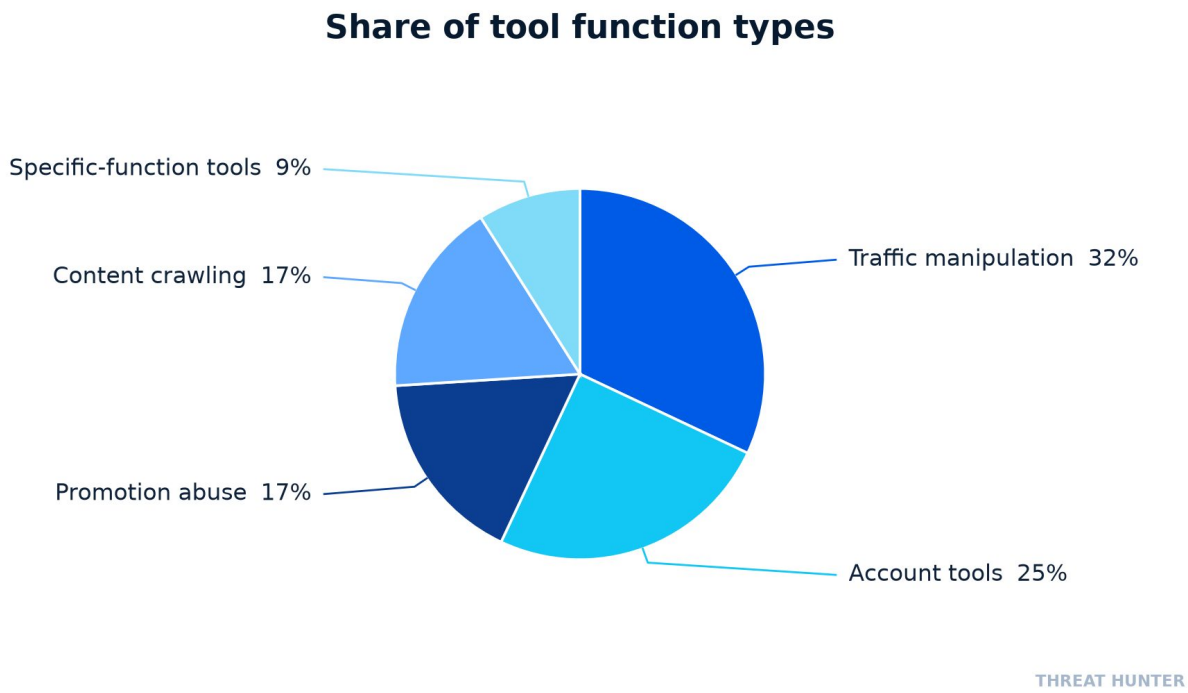


Figure 3-1: share of tool function types; traffic manipulation tools are the largest group

Source: Threat Hunter original report, page 17. Redrawn in English from the original figure.

3.1 Account tool software

In most threat actors chains, the quality and quantity of accounts largely determine the input-output ratio of threat actors. Account tool software is mainly aimed at registration scenarios and login scenarios, and the functions implemented include batch registration, account scanning, authentication and unauthorized access, etc. Take a registration and number-scanning tool as an example. This tool is directly connected to the SMS verification-code receiving service and is used to receive SMS verification codes. At the same time, the built-in VPS dial-up function is used to bypass the company's IP restriction policy, thereby completing batch registration and number scanning of accounts.

Account type 25% volume and order traffic manipulation type 32% promotion abuse type 17% content crawling type 17% specific function type 9% account type traffic manipulation volume and order type promotion abuse type content crawling type specific function type

Figure 3-1-1 Registration and account-scanning software The profit-making methods of account-type tool software include: 1. Directly selling batch-registered accounts to external parties, and there is a certain distribution system for account sales, and agents of different levels have different prices; 2. By using batch-registered accounts in business scenarios such as traffic manipulation up volume and attracting traffic, such as messaging, email and social media accounts. Some accounts can be used to authorize services for other companies' businesses. This type of account is called a jump account, and the cost of jump accounts is low; 3. A batch of customized accounts for company promotion activities, combined with the SMS verification-code receiving service, CAPTCHA-solving service, etc. to complete fully automated fraud operations, and collect a large number of user bonuses in a short period of time. Nowadays, the cybercrime ecosystem business chain with account as the core has developed to a certain scale in various industries, especially in business scenarios that require large-scale account traffic manipulation, including false registration, real-name face recognition, batch account maintenance and traffic manipulation, etc. In addition to the obvious harm to the company's business, there is also the potential harm caused by false trumpets. For example, the spread of pornography, gambling, and drugs, as well as its use in traffic fraud scenarios, have brought negative public opinion effects to companies. The following table shows some of the more active account tools and software that we have monitored recently: Table 3-1-1 Active account tools: a cracked PC cloud-drive client (high), a cloud-drive download accelerator (high), a news-app account registration bot (medium), a video-streaming membership scanner (medium) and an account-scanning query tool (medium).

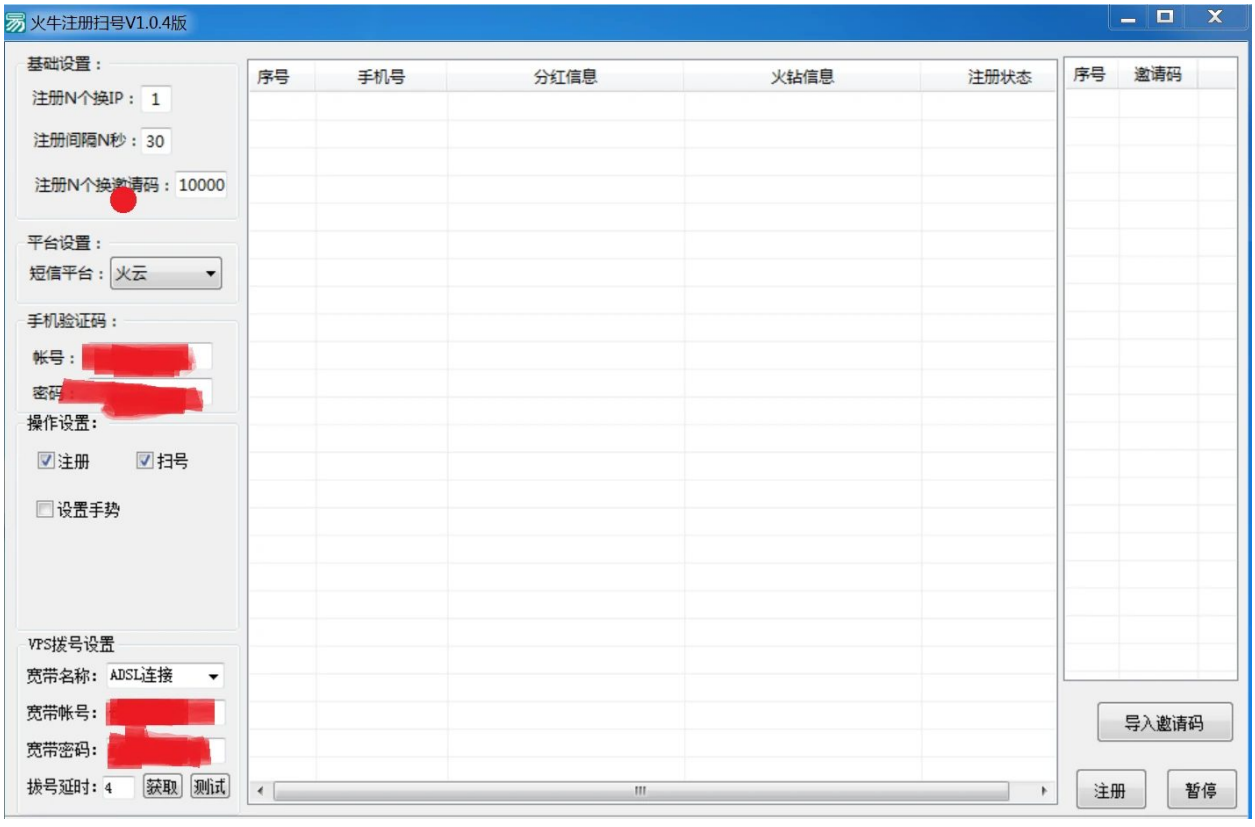


Figure 3-1-1: registration and account-scanning software

Source: Threat Hunter original report, page 18. Original screenshot retained.

3.2 Volume traffic manipulation tool software

Volume and order traffic manipulation tools and software are mainly active in e-commerce, self-media, short video and other industries. Its main functions include traffic manipulation transaction volume, traffic manipulation reading volume, traffic manipulation playback volume, traffic manipulation attention volume, traffic manipulation fan volume, traffic manipulation comment volume, etc. Take a play-count boosting tool for a short-video platform as an example. The tool first loads a batch of tokens for bulk-registered accounts, and then simulates network requests to access the URL of the target short video, and finally can successfully manipulate the playback volume.

Figure 3-2-1 Short-video play-count boosting tool The profit-making methods of tools and software for traffic manipulation orders include: 1. Charging commissions from task publishers by providing volume traffic manipulation and order traffic manipulation services; 2. In response to the freight subsidies subsidized by e-commerce platforms for merchants, by combining empty package logistics services, initiating return requests to collect subsidies; 3. Combining likes and traffic manipulation comments, placing top comments under user works, generating followers through personal introductions or comment content, and the price of followers is calculated based on the number of accounts introduced to other platforms, etc. The following table shows some of the more active tools and software for traffic manipulation orders that we have monitored recently: Table 3-2-1 Active order traffic manipulation tools: short-video follower boosting software (medium), a news-app follow, message and comment tool (high), an empty-parcel website (medium), group-buying assist software (medium), fully automatic fake-order software for a marketplace (medium) and automatic fake-order software for a group-buying platform (medium).



Figure 3-2-1: a play-count boosting tool for short-video accounts

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

3.3 Promotion-abuse tool software

Promotion-abuse tool software is mainly active in marketing activities, e-commerce rush purchases, red envelope collection and other scenarios. Take "WALL-E Grab Red Envelope" as an example. This tool activates auxiliary functions and simulates clicking controls to achieve functions such as grabbing red envelopes and automatic replies.

Figure 3-2-2 A red-envelope grabbing tool. The profit-making methods of promotion abuse tool software include: 1. Directly selling the tool software to make a profit; 2. Using the tool to receive coupons or red envelopes launched by the platform, or reselling coupons, red envelopes, etc.; 3. Selling the purchased items a second time to earn the price difference, etc. The following table shows some of the more active promotion abuse tools and software that we have monitored recently: Table 3-2-3 Active promotion abuse tools: e-commerce snap-up software V3.06 (medium), a free-trial application tool V1.0 (medium), rush-buy order software 1087 (high), a red-envelope monitoring tool for a flash-sale channel, and coupon checking and collection software 545 (medium).



Figure 3-2-2: settings of a red-envelope grabbing tool, such as auto-grab, delay and keyword filters

Source: Threat Hunter original report, page 20. Original screenshot retained.

3.4 Content crawler tool software

Content crawler tool software mainly collects e-commerce data, short video user works, recruitment website resumes and self-media articles through crawler programs. Recently, we have discovered that there are many tools and software that crawl a group-buying platform's product, store and group information. Taking one such crawler as an example, it collects the platform's data by calling its public API, and provides functions such as group opening reminders, keyword rankings, category rankings, export orders, logistics monitoring, refund reminders, and competitor monitoring:

Figure 3-2-3 and Figure 3-2-4 Screenshots of the crawler The profit-making methods of content crawling tool software include: 1. Use the collected platform data to provide data analysis



Figure 3-2-3: a content crawler collecting user records into a table

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



Figure 3-2-4: a crawler collecting recruitment and listing data

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

Profitable analysis services and store management services, including keyword ranking, product ranking, group opening monitoring, one-click ordering, one-click shipping and multiple store management, etc.; 2. When stores use these tools, it is likely to lead to order data leakage, and cybercriminal groups can make profits by selling these data or using the data for marketing and fraud. The following table shows the relatively active content crawling tools and software that we have monitored recently: Tool name Activity level Duoduo Guanjia High Duoduo Consultant High McDull/Shoujie/Benben Daigou Medium Duoduo Yizan Medium Shenma Huo Assistant Medium Table 3-2-4 Content crawling tools

3.5 Tool software with specific functions

Specific functional tool software mainly includes functional tool software such as emulators, multi-opens, computer modifications, and instant dials. It is commonly used in scenarios such as registering accounts, inviting new users to receive red envelopes, boosting likes, boosting shares, boosting ratings, and boosting rankings. There are not many types and quantities of tool software with specific functions, but they also play an extremely critical role in the cybercrime ecosystem chain. Take one device-modification tool as an example. When diverting traffic from a short-video app, the modified device can be used to fake the location, use the app's nearby-videos feature to divert traffic, and induce nearby people who see the video to add a messaging-app contact.

Figure 3-5-1 Figure 3-5-2 As shown above, the location is changed to a busy railway station with the help of the modification software, and then "carefully" produced videos or pictures of beautiful women are uploaded to the short-video app with text containing messaging-app IDs. Finally, the hooked male users are directed to messaging-app merchants selling men's products, or are

induced to give red envelopes to watch pornographic videos, and are eventually deceived. Although tool software with specific functions does not participate in direct profit-making, the functions provided can help the cybercrime ecosystem better obtain profits. For example, the machine modification tool, in addition to the traffic diversion scenarios mentioned above, is also very important in the account registration scenario, which can achieve the effect of reusing a device multiple times. The following table shows the relatively active specific function tool software that we have monitored recently: Table 3-5 Active specific function tools: five device-modification tools, one with high activity and four with medium activity.



Figure 3-5-1: device location before using location-changing software

Source: Threat Hunter original report, page 23. Original screenshot retained.



Figure 3-5-2: the location changed to a busy railway station with the modification software

Source: Threat Hunter original report, page 23. Original screenshot retained.

4. Analysis of typical cybercrime ecosystem tool software In the past six months, we have done a lot of research and analysis on cybercrime ecosystem tool software, including in-depth functional verification, dynamic debugging and principle analysis of some of the tool software. We select several typical software tools to further reveal their functions and principles.

4.1. Mobile registration bot 3.0 for a video community

This is a registration tool for a video community platform, captured in June and written in C++ language. By using the phone number of the SMS verification-code receiving service to receive the mobile phone verification code, and the built-in deep learning framework Caffe to recognize the image verification code, complete account batch registration. The program running interface is as shown below:

Figure 4-1-1 The running interface of the registration bot. The program will log in to the SMS verification-code receiving service: http://www.7gxyun.com:9000/soft.html to receive the SMS verification code, and then call the platform's phone registration interface and its image-CAPTCHA interface to extract the verification code, as shown below:

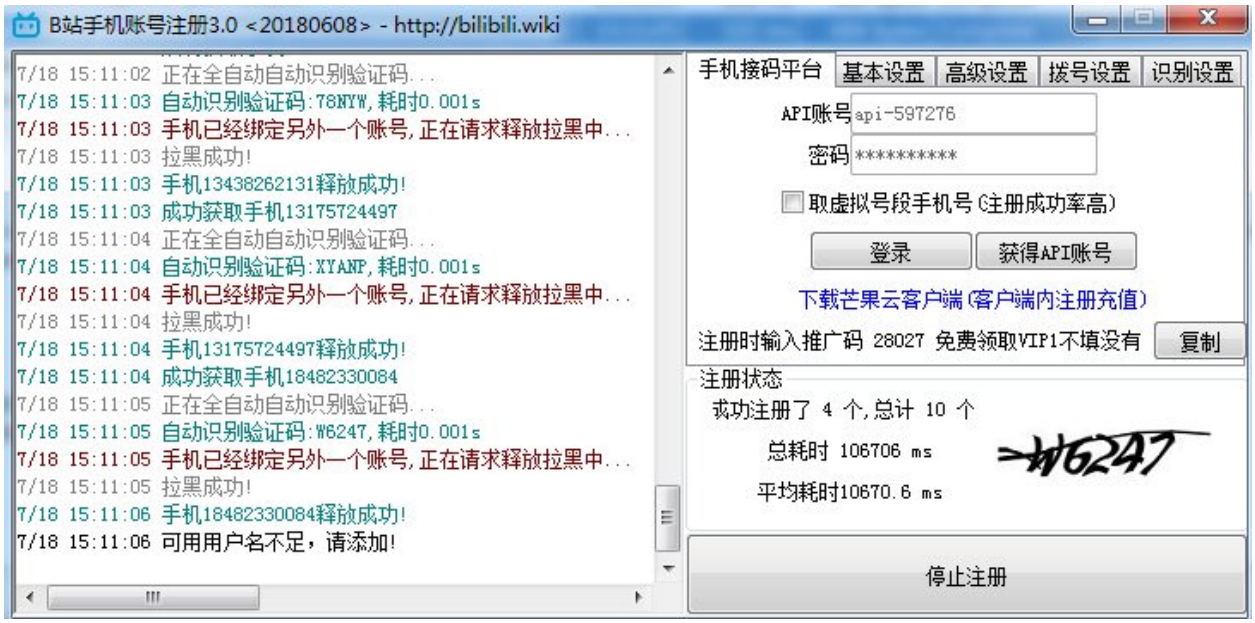


Figure 4-1-1: running interface of the registration bot for a video community

Source: Threat Hunter original report, page 24. Original screenshot retained.

The tool then uses the built-in deep learning framework Caffe to recognize the image verification code. The process of identifying the verification code will read three files required by the local built-in deep learning framework Caffe framework: deploy.prototxt, res_lstm_ctc_iter.caffemodel, label-map.txt. Part of the code of deploy.prototxt is as follows:

Figure 4-1-2 screenshot of deploy.prototxt code. After the image verification code is successfully recognized, the account registration is completed. The highlight of this tool, which is different from the tools we have seen in the past, is that it uses the image recognition capability of deep learning, and the accuracy of this image recognition reaches more than 99%, and the average time to complete the registration of an account is about 10 seconds. In the past, most registration tools of this type were connected to a CAPTCHA-solving service or built-in a verification code recognition library for the target website. Both the recognition accuracy and the registration efficiency were much lower than those using deep learning image recognition.

deploy.prototxt: CAPTCHA recognition model

```
name: "Res LSTM CTC"
input: "data"
input_shape {
  dim: 1
  dim: 3
  dim: 50
  dim: 200
}
layer {
  include { phase: TEST }
  name: "indicator"
  type: "ContinuationIndicator"
  bottom: "data"
  top: "indicator"
  continuation_indicator_param { time_step: 25  batch_size: 1 }
}
# Notes: dim 1 = number of augmented copies of each sample to recognize
#        dim 3 = image channels (RGB)
#        dim 50 = image height; dim 200 = image width
# res_lstm_ctc_iter.caffemodel: the already-trained model file
```

THREAT HUNTER

Figure 4-1-2: the deploy.prototxt model definition used to recognize image CAPTCHAs

Source: Threat Hunter original report, page 25. Text re-typeset in English from the original screenshot; identifiers shortened.

Figure 4-1-3 Deep learning applied to verification code recognition

4.2. Red-envelope grabbing tool for a social app

This is a red-envelope grabbing tool for a social app, captured in July and based on the Android version of a popular automation appzard. By customizing the recording of information such as the operation of the mobile phone screen and the number of repetitions, the mobile phone can be simulated according to a certain pattern to achieve functions such as grabbing red envelopes. The tool runs as shown below:

Figure 4-2-1 Running interface of the red-envelope grabbing tool

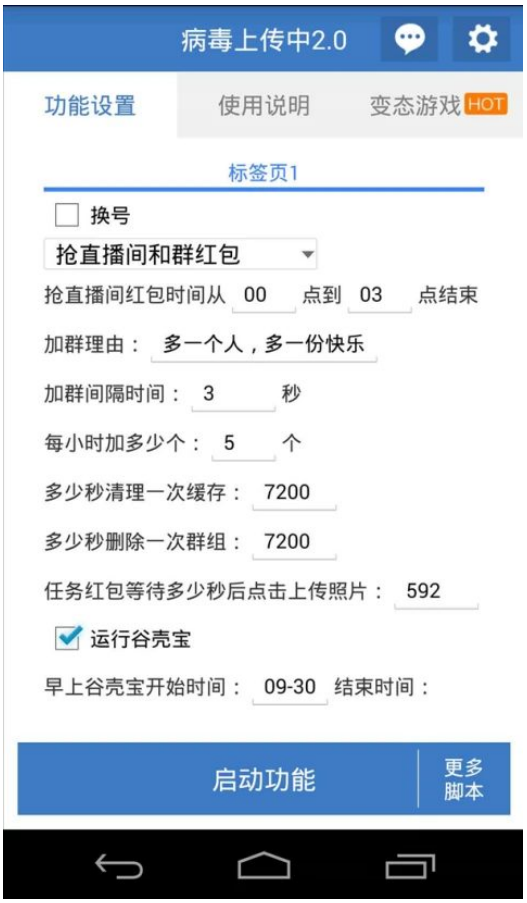


Figure 4-2-1: running interface of the red-envelope grabbing tool

Source: Threat Hunter original report, page 26. Original screenshot retained.

cybercrime operators only need to write relevant logic scripts on the automation app's Android version to simulate user operations to achieve the functions they want. The operating interface of the automation app is as shown in the figure below:

Figure 4-2-2 Automation app running interface After clicking "Record", the user can first manually operate the function he wants to operate, and then the software will record the coordinate trajectory of the user's operation, as shown in the figure below:

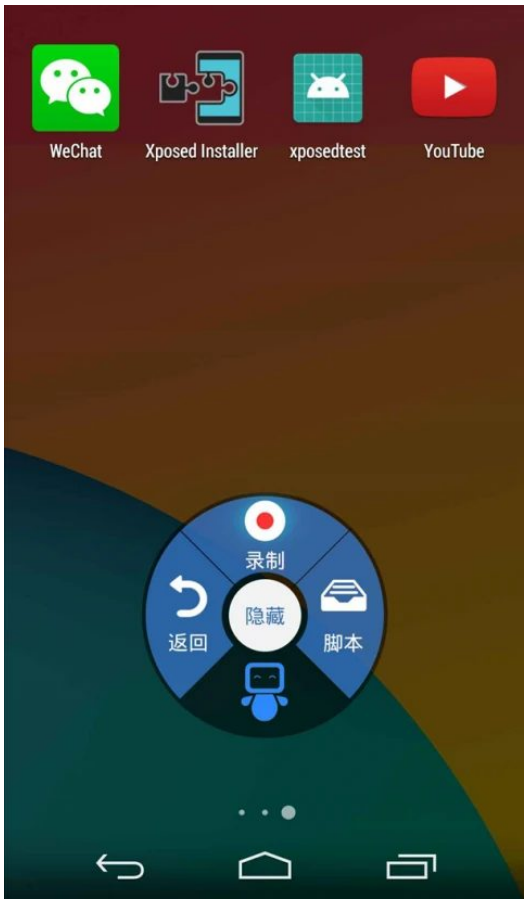


Figure 4-2-2: the automation app's floating menu for recording, playing back and running scripts

Source: Threat Hunter original report, page 27. Original screenshot retained.

Figure 4-2-3 Automation app running interface

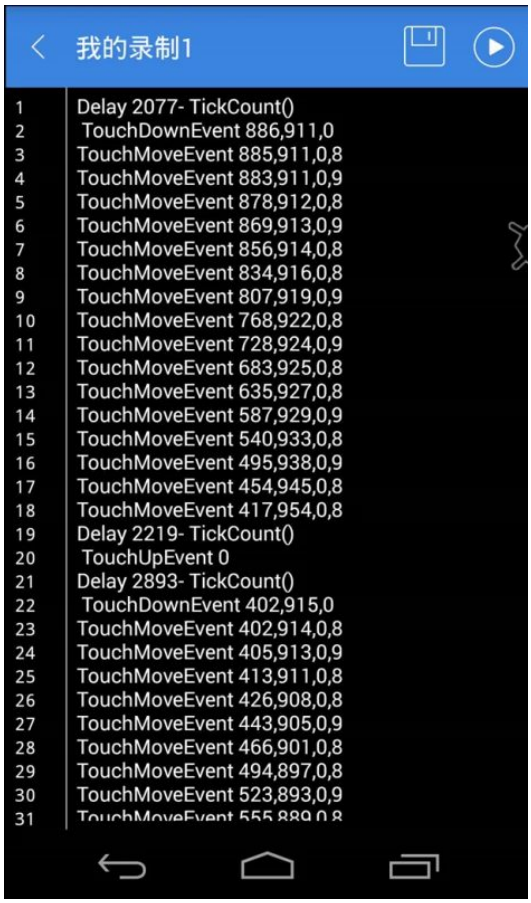


Figure 4-2-3: a recorded script of touch coordinates, actions and delays that the app replays

Source: Threat Hunter original report, page 27. Original screenshot retained.

During our analysis, we found that the red envelope grabbing tool has some built-in resources needed by the tool, including identifying images when red envelopes appear, as shown in the figure below:

Figure 4-2-4 The built-in image resources of the red-envelope grabbing tool. The software runs in the background, searching for the coordinates of the above screenshot image on the entire phone screen, and then simulating the user’s click operation to achieve the purpose of grabbing red envelopes.



Figure 4-2-4: built-in image resources the tool matches on screen to find buttons

Source: Threat Hunter original report, page 28. Original screenshot retained.

4.3. Full-time VIP posting software for a classifieds site

This is an automatic posting tool software for a classifieds site, captured in August. The principle of this tool is to crack the site's posting interfaces. When calling the relevant interface, the software will splice together the parameters required by the interface and then request it from the server. The interfaces implemented in the software include: login, posting, obtaining displayed posts, undisplayed posts, deleted posts, reviewing posts, obtaining unread resumes, etc. We use the post function to illustrate the working principle of the software, and other interface calls are similar. The interface for running this tool software is shown in the figure below:

Figure 4-3-1 Running interface of the VIP posting software There will be many posting-related settings on the interface. These settings were extracted by cybercrime ecosystem staff after analyzing the site's posting interface. Some variable values □□that the user needs to operate (including some parameters required by the interface such as province, city, street, post title, post position, etc.). The following is the interface information captured by our constructed VIP users posting recruitment posts:

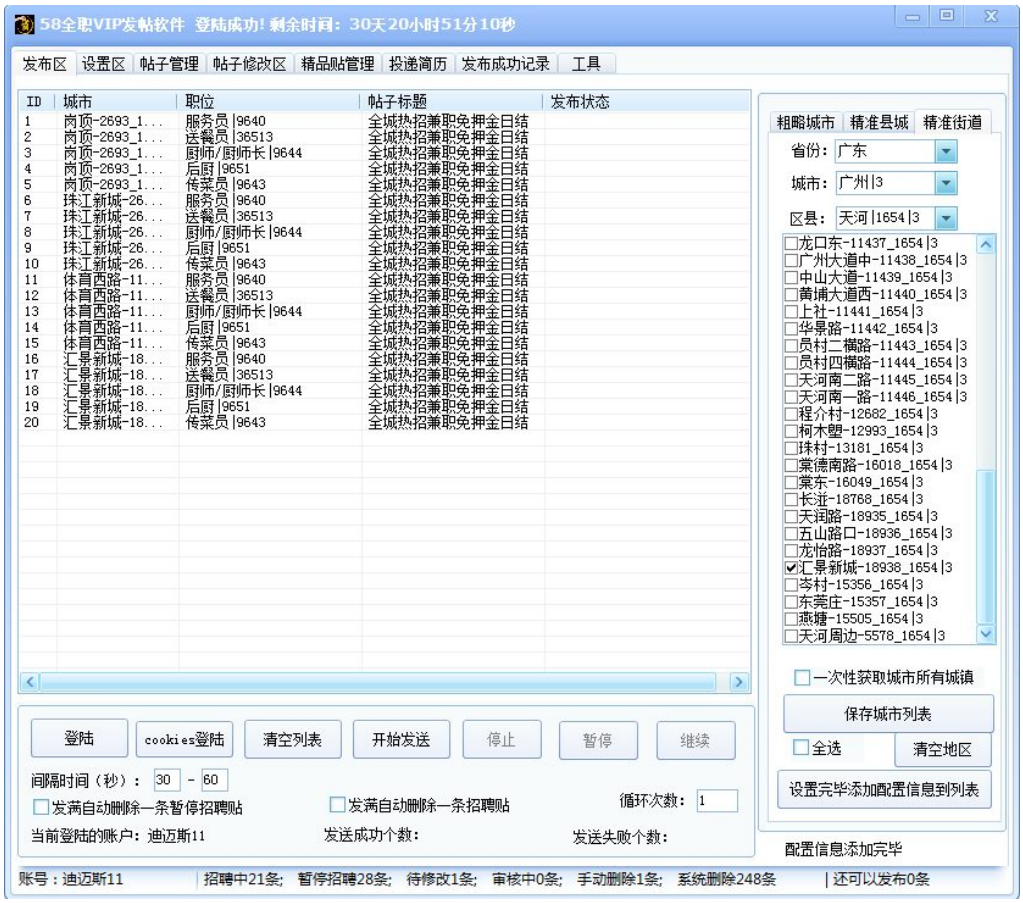


Figure 4-3-1: running interface of the VIP posting software for a classifieds site

Source: Threat Hunter original report, page 29. Original screenshot retained.

Figure 4-3-2 Captured interface information The following is the content that needs to be POSTed by the interface (since the data is encoded by UrlEncode, for the convenience of reading, the plain text data before encoding is displayed):

Captured posting request (abridged)

```
POST /zhaopin/771/9640/s5/submit HTTP/1.1
Referer: http://[posting host]/zhaopin/771/9640/s5/submit:1080
Accept-Language: zh-cn
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Origin: https://[posting host]
Cookie: PPU="UID=5621682304…&UN=…&TT=…&PBODY=…&VER=1"; post_uuid=…; id=…;
        deviceid=…; smartid=…; sessionid=…; gr_user_id=…;
        cooper="userid=5621682304…&username=…&cooperkey=…";
        site="AutoLogin=false&UserID=5621682304…&UserName=…&SiteKey=…";
        vip=vipusertype=11&vipuserpline=0&v=1&vipkey=…&masteruserid=5621682304…;
        PPStore_fingerprint=…
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
            like Gecko) Chrome/55.0.2883.87 Safari/537.36
Accept: */*
Host: [posting host]
Content-Length: 2465
```

THREAT HUNTER

Figure 4-3-2: the captured posting request (host and cookie values shortened)

Source: Threat Hunter original report, page 30. Text re-typeset in English from the original screenshot; identifiers shortened.

Figure 4-3-3 POST data content (before encoding) We can see that most of the above content is information filled in by users. As long as the same form data is constructed according to the posting interface format, the post can be successfully posted. We can see from the relevant parameters required by this interface that the 58VIP posting interface requires a lot of parameters, which requires cybercrime operators have strong protocol interface analysis capabilities and can analyze which parameters are necessary, which parameters are dispensable, which parameters must be detected by the fraud-control system, and whether the parameter values □□are encrypted. If it is encrypted, cybercrime operators need to crack the encryption algorithm and then calculate new parameter values □□to bypass the detection of the fraud-control system. Except for the above-mentioned posting interface, the forms of other interface calls are similar to the above.

POST data before encoding (Chinese values translated)

```
title=City-wide hiring of part-time staff, daily pay, free food and housing
&jobcateID=13915&personnumber=10&eduid=1&experienceid=1&yingjiesheng=1
&salary=5000_8000
&content=Who are we?
   A Guangzhou catering management consultancy running all kinds of food
   businesses: university canteens, 5-star hotels, seafood markets, street
   food stalls and trending restaurants. As the business grows we are
   hiring: women aged 18-32, height 160 cm or above;
   men aged 18-35, height 170 cm or above. Experience not required; training
   provided. Apply online or call. We look forward to you joining us!
&disablecheck=off&welfareid=1|10|8|9|4|2|7
&welfarestring=social insurance|meals|housing|year-end bonus|housing and meal
   allowance|overtime pay
&contact=Lilith&phone=1326688****&showphone=1&email=2034254642@[mail domain]
&localcityid=3&localareaid=1654&localdiduanid=2693&addressid=10699378
&isshowjz=false&captcha_input=&yzm=&cateid=9640&captcha_responseid=
&captcha_encryptedKey=&userid=5621682304…&jz_refresh_post_key=0
&captcha_type_message=400
```

THREAT HUNTER

Figure 4-3-3: POST data content before encoding, translated

Source: Threat Hunter original report, page 31. Text re-typeset in English from the original screenshot; identifiers shortened.

5. Conclusion cybercrime ecosystem tool software is an inevitable product of the development of the cybercrime ecosystem. cybercriminal groups will develop with the development of the Internet, and cybercrime ecosystem tool software will also develop with the development of the cybercrime ecosystem. Based on this, we put forward the following opinions, hoping to resonate with the industry and discuss and think with everyone. 1. From the perspective of threat actors, build comprehensive monitoring and rapid response capabilities for cybercrime ecosystem tool software. Through long-term follow-up of the cybercrime ecosystem, we have a relatively in-depth understanding and knowledge of the transmission chain and path of the cybercrime ecosystem tools. We can capture active the cybercrime ecosystem tools on the network as soon as possible, and analyze their harm and principles at the first time. We hope to help more companies build capabilities in this area through cooperation. 2. Establish a fingerprint database for cybercrime ecosystem tool software to enhance the identification capabilities of risky equipment. Traditional device fingerprinting solutions are not ideal for identifying risky devices due to fierce confrontation; on the other hand, risky devices are often installed with a variety of cybercrime ecosystem tool software. By extracting the characteristics of these cybercrime ecosystem tool software as fingerprints, risky devices can be effectively identified. 3. Establish cybercrime tool software intelligence sharing in the industry to maximize the value of intelligence. According to our observations, there is overlap among the authors, communication channels, and users of tool software. Taking e-commerce rush buying as an example, when we followed rush-buying tools for

one major marketplace, we found that many of their users also use rush-buying tools for several other online malls to maximize profits. That is, the cybercrime ecosystem tool software fingerprint library we mentioned in point 2 can actually be shared by the industry, and we have been committed to solving the data island problem of cybercrime ecosystem intelligence, including tool software intelligence. Written at the end: If cybercrime ecosystem represents the dark night, only by constantly exploring and moving forward in the dark night can we usher in the light and encourage you all.

Note 1. Data source description: The data in this report comes from the Threat HunterTH-Karma business intelligence monitoring platform. The sampling mainly adopts "keyword sampling", "similarity sampling" and "stratified sampling" methods. There may be certain deviations between the data analysis results obtained based on the above data sampling methods and the actual situation. Please understand. 2. Description of the business intelligence monitoring platform: The business intelligence monitoring platform - TH-Karma, from the perspective of an attacker, relies on powerful cybercrime ecosystem control capabilities and deep intelligence processing capabilities to help enterprises accurately screen out malicious traffic in business links, restore business risk scenarios, and quantify the impact on the business. It also continuously monitors threat actors in real time, drives the iteration of the fraud-decision engine, and thereby improves the overall offensive and defensive efficiency of the enterprise.

Welcome to follow the Threat Hunter official account to get more professional reports