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.

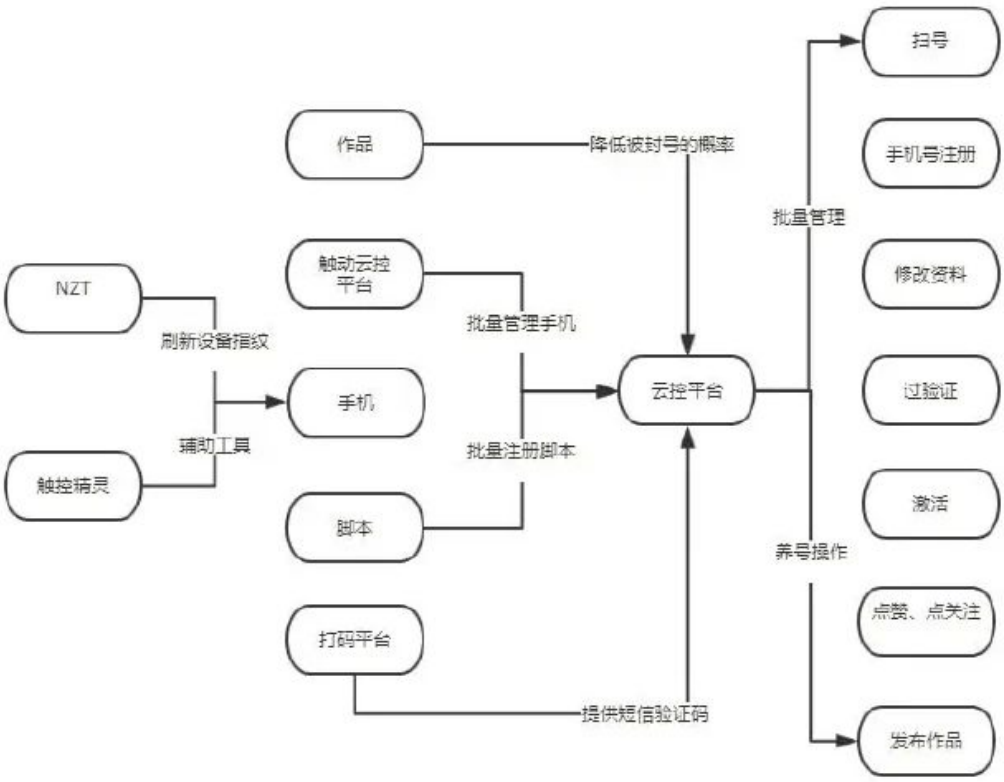
Original publication: 2018-07-31
Research team: Threat Hunter Research Team
Source report: 33 pages

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.

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.



Changers, codekeeping, cloud control, scripts and batch management tools together constitute automated account workflows.

Source: Threat Hunter original report, page 3

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 Jingdong's registration machine tool software 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] Jingdong registration v18.0105.rar January 9, 2018 [Registration client] Jingdong registration v18.0109.rar January 18, 2018 [Register Client] JD Registration v18.0118.rar January 19, 2018 [Register Client] JD Registration v18.0119.rar January 21, 2018 [Register Client] JD Registration v18.0121.rar January 30, 2018 [Register Client] JD Registration v18.0130.rar

February 26, 2018 [Register Client] JD Registration v18.0226.rar March 19, 2018 [Register Client] JD Registration v18.0319.2.rar March 21, 2018 [Register Client] JD Registration v18.0321.rar March 22, 2018 [Register Client] JD Registration v18.0322.rar April 7, 2018 [Register Client] JD Registration v18.0407.rar April 11, 2018 [Register Client] JD Registration v18.04011.rar April 11, 2018 [Register Client] JD Registration v18.04011.2.rar April 15, 2018 [Register Client] JD Registration v18.04015.rar April 18, 2018 [Register Client] JD Registration v18.0418.rar April 20, 2018 [Register Client] JD Registration v18.0420.rar April 25, 2018 [Register Client] JD Registration v18.0425.rar April 25, 2018 [Register Client] JD Registration v18.0425.2.rar April 26, 2018 [Register Client] JD Registration v18.0426.rar April 27, 2018 [Register Client] JD 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:

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

出现了一些薄弱点，很快就会出现利用此来攫取利益的工具软件，其中以针对营销活动的薅羊毛工具软件最为典型。美团在 18 年俄罗斯世界杯前夕推出了看球竞猜活动：

活动推出后不久，网络上就出现了 50 款以上针对该活动的工具软件，跟美团业务

There's a remarkable trend towards profit.

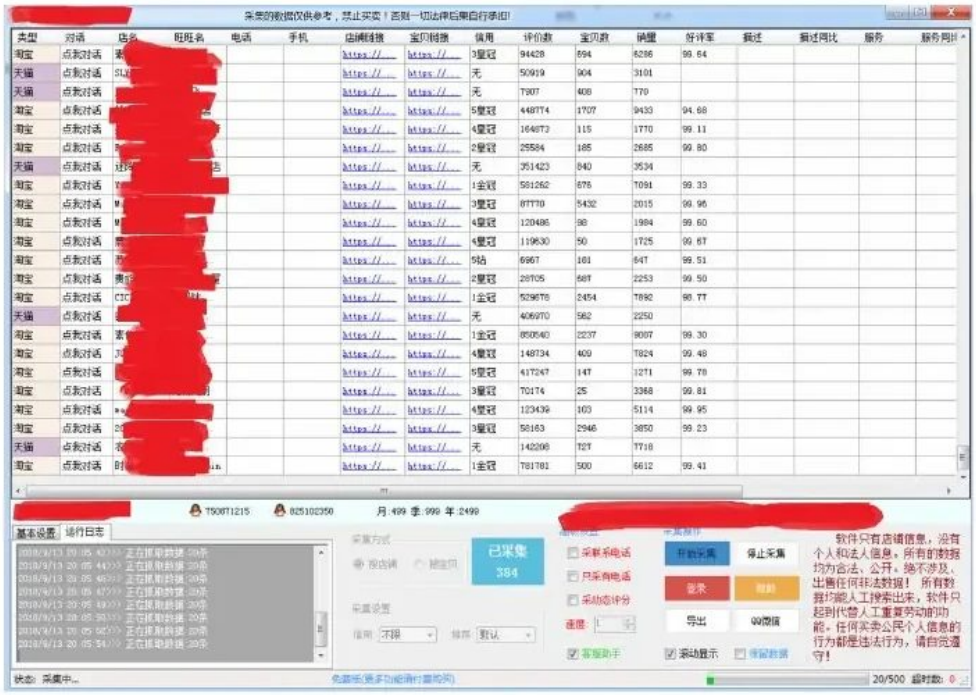
Source: Threat Hunter original report, page 8

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.

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

店铺引流等功能。有些软件还在界面显著位置放置了免责声明（虽然不一定有用），如下图：



当然，随着法律的不断健全和完善，目前认为是法律边缘的“灰色”地带，未来某

Swim in the grey zone on the edge of the law.

Source: Threat Hunter original report, page 9

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, tool software for Tencent business needs to log in to QQ or WeChat first, and tool software for Alibaba business needs to log in to Taobao first), 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. I spent a lot of money to buy so-called awesome tools, such as "100% modification of machine code", "VIP member crack", "fully automatic flash sale", etc., but after using them, I found 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. Therefore, I would like to 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 Baidu Netdisk, 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

Out of its core code logic, the following figure is a code fragment that splices the Baidu Netdisk 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.baidu.com/rest/2.0/pcs/file?method=download&app_id=250528&path=" + encodeURIComponent(e[n].path), md5: e[n].md5 }); return Promise.resolve() }

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 Button Wizard Android version 0500100015002000250030003500400045000 Douyin Kuaishou Momo PC/Mobile Tool Software Number Comparison between PC and Mobile

The cybercrime ecosystem tool written by Heyi Android covers the core business scenarios of cybercrime ecosystem such as registration, traffic manipulation, and traffic diversion, as shown below:

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:

```
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.baidu.com/rest/2.0/pcs/file?method=download&app_id=250528
&path=" + encodeURIComponent(e[n].path),
                        md5: e[n].md5
                    });
```

The core code of the tool is a 100-degree web download request link based on the file path.

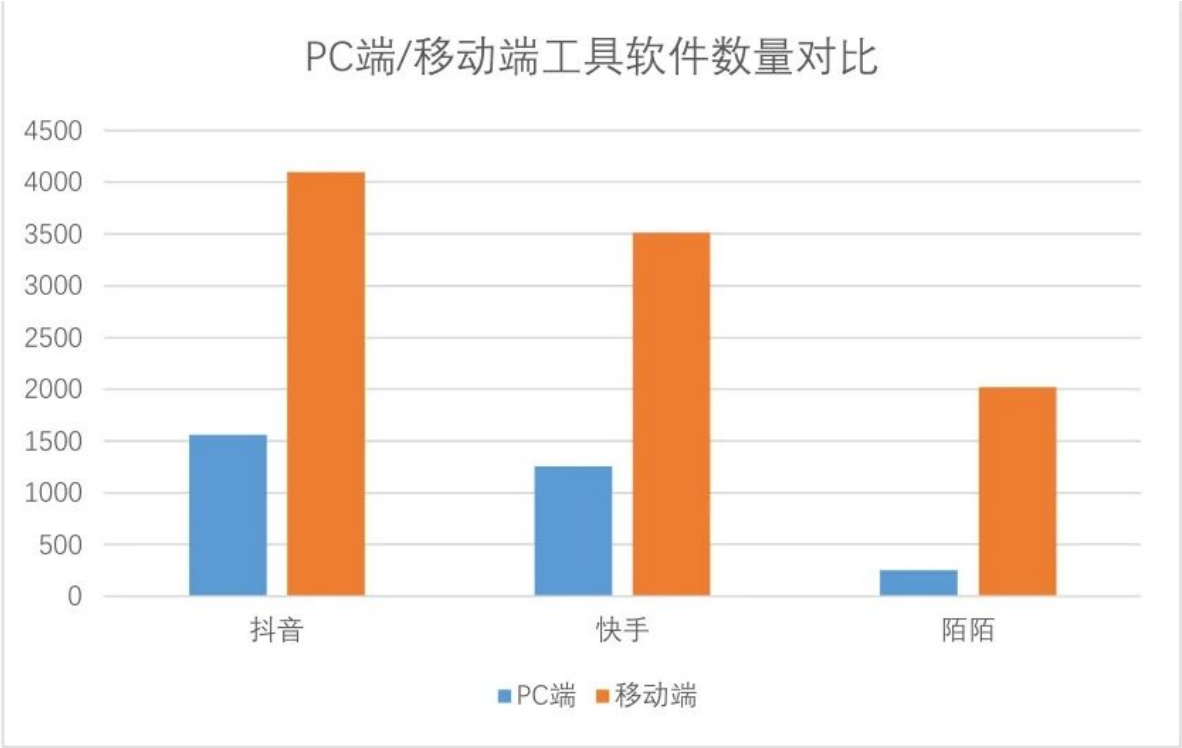
Source: Threat Hunter original report, page 12

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:

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.

2.4 From mechanical execution to machine learning



In the monitoring sample, the number of mobile cybercrime-producing tools at the vibrating, fast-hand and strange end was significantly higher than at the PC end.

Source: Threat Hunter original report, page 13

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:

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.

注册机	陌陌批量注册2018-05-01_015811.apk
注册机	陌陌批量注册2018-05-01_134610.apk
注册机	陌陌批量注册2018-05-01_170054.apk
注册机	陌陌批量注册2018-05-09_103551.apk
注册机	陌陌批量注册2018-05-10_130412.apk
注册机	陌陌批量注册2018-05-16_155650.apk
刷量	陌陌评论1.02018-04-09_024220.apk
刷量	陌陌评论1.22018-04-09_195258.apk
刷量	陌陌评论1.52018-04-14_193518.apk
引流	陌陌群组引流2018-05-17_163550.apk
引流	陌陌群组引流2018-05-17_172801.apk
刷量	陌陌刷直播间1.02018-03-18_160047.apk
刷量	陌陌刷直播间1.32018-03-18_200441.apk
刷量	陌陌刷直播间1.32018-03-18_200441.apk(1).1
引流	陌陌引流2018-01-27_195531.apk
引流	陌陌引流2018-05-11_002728.apk
引流	陌陌引流2018-05-11_111238.apk
引流	陌陌引流2018-05-13_101822.apk
引流	陌陌引流3.02018-03-15_234312.apk
引流	陌陌引流3.92018-04-02_174144.apk
引流	陌陌引流4.12018-04-13_142437.apk
引流	陌陌引流4.22018-05-15_150425.apk
引流	陌陌引流4.22018-05-15_150425.apk
引流	陌陌引流4.32018-05-16_060243.apk
引流	陌陌引流v4.02018-04-06_225322.apk
引流	陌陌引流-飞缘-4.22.apk
引流	陌陌引流脚本2018-03-18_172620.apk
引流	陌陌引流脚本4.102018-04-10_223129.apk
引流	陌陌引流脚本4月18号.apk
引流	陌陌引流脚本正式版.apk
引流	陌陌引流软件2018-03-14_223954.apk

Samples show that mobile end tools cover core scenarios such as account number registration, traffic manipulation and diversion.

Source: Threat Hunter original report, page 14

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.

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 "Huoniu Registration and Number Scanning Software" 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.

图 2

From terminal to cloud

Source: Threat Hunter original report, page 14

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 Huoniu 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 QQ, email, The Weibo account itself 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: Tool name Activity Baidu Cloud PC Cracked Version High PanDownload High Toutiao Account Registration Machine Medium iQiyi Member Scanner Medium Huoniu Account Scan Query Medium Table 3-1-1 Active account tools

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 "Jiujiu Kuaishou manipulate Playback" as an example. The tool first loads a batch of Kuaishou trumpet tokens in batches, and then simulates network requests to access the designated Kuaishou work URL, and finally can successfully manipulate the playback volume.

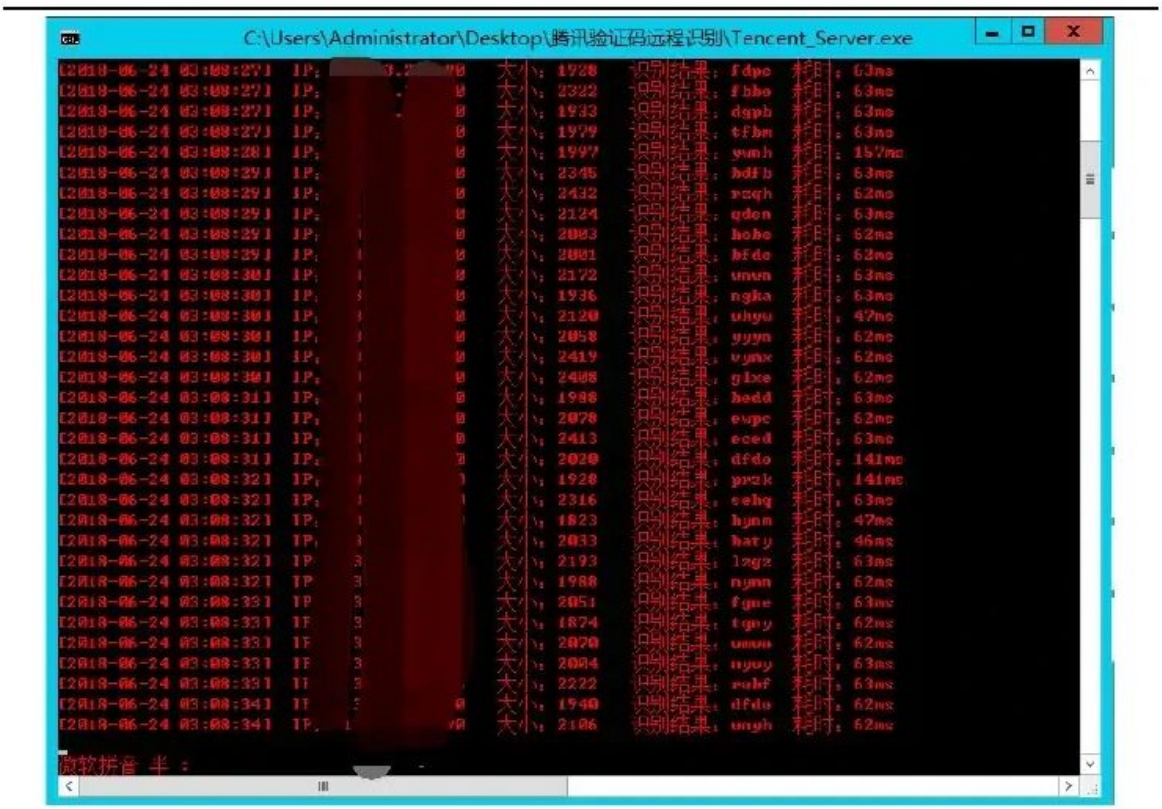


图 3.2

From mechanical execution to machine learning.

Source: Threat Hunter original report, page 16

Figure 3-2-1 Jiujiu Kuaishou manipulate Play 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: Tool name Activity level Kuaishou fan traffic manipulation software Medium Toutiao (follow + private message + comment) High Zhaocai empty package website Pinduoduo assistance Medium Taobao fully automatic order traffic manipulation software Medium Pinduoduo automatic order traffic manipulation software Medium Table 3-2-1 Active order traffic manipulation tools

3.3 Promotion-abuse tool software

From mechanical execution to machine learning.
Source: Threat Hunter original report, page 17

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 Vali grabs red envelopes. 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: Tool name Activity level Blade JD snap-up software V3.06 Medium JD Application for Trial (Pulling Real Things) V1.0 Medium JD Huoniu-order rush-buy software 1087 High Juhuasuan Red Envelope Monitoring JD Huoniu-coupon checking and collection software 545 Medium Table 3-2-3 Active promotion abuse tools

3.4 Content crawler tool software

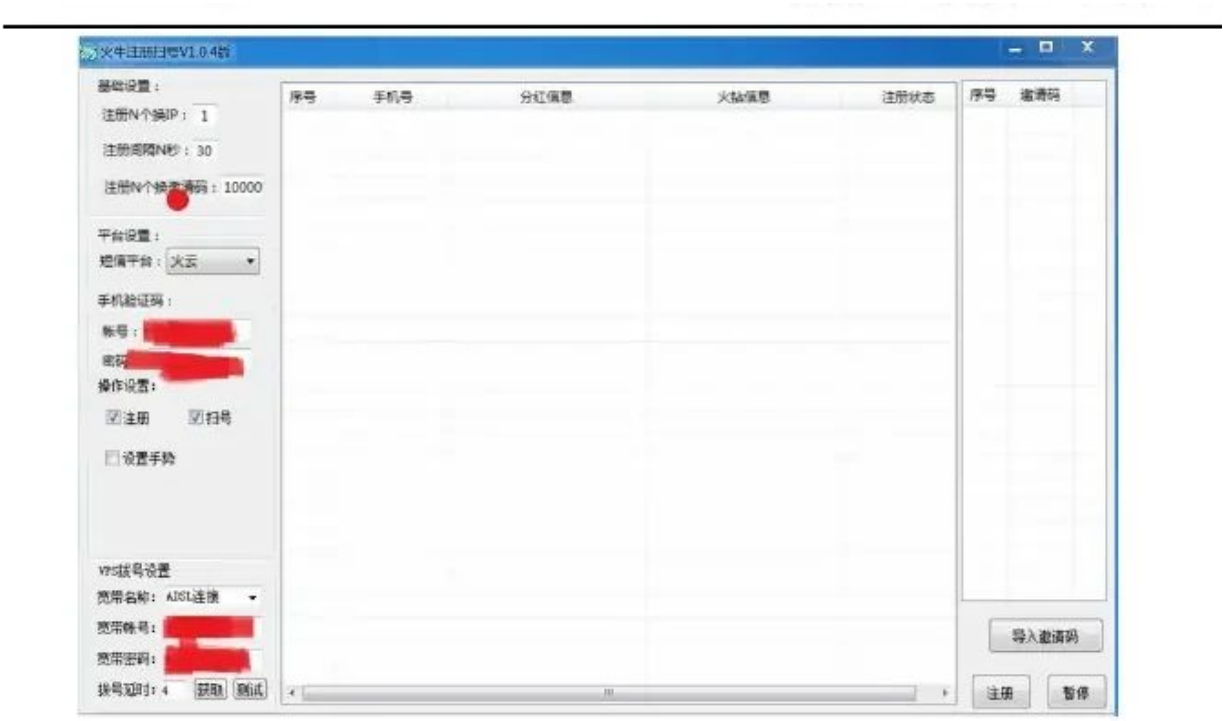


图 3-1-1 火牛注册扫号软件

Account-type tool software

Source: Threat Hunter original report, page 18

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 Pinduoduo's product information, store information, group information and other data. Taking "Pinduoduo Elf" as an example, this tool software crawls Pinduoduo data by requesting the interface under apiv4.yangkeduo.com, 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 Screenshot of Pinduoduo Elf 1 Figure 3-2-4 Screenshot of Pinduoduo Elf 2 The profit-making methods of content crawling tool software include: 1. Use the collected Pinduoduo data to provide data analysis

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 the modification software "Haiyu Magic Device" as an example. In the scenario of diverting traffic to Douyin, the modified device can be used to fake the location, use the function of nearby videos on Douyin to divert traffic, and induce nearby people who see the video to add a WeChat account.

Brush List Tool Software

Source: Threat Hunter original report, page 19

Figure 3-5-1 Figure 3-5-2 As shown above, the location is changed to the Guangzhou Railway Station with a lot of traffic with the help of the modification software, and then "carefully" produced videos or pictures of beautiful women are uploaded through Douyin, accompanied by text containing WeChat IDs. Finally, the hooked male users are directed to WeChat 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: Tool name Activity Deep Sea Fish Music Medium iGrimace High 007 Modification Medium NTZ Medium AWZ Medium Table 3-5 Active specific function tools

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.Bilibili mobile registration machine 3.0

嫣丰毛类工具软件主要活跃于营销活动、电商抢购、红包领取等场景。以“瓦力抢红包”为例，该工具通过开通辅助功能，模拟点击控件从而实现抢红包及自动回复等功能。

图 3-2-2 瓦利抢红包

Example of a tool used to automate promotion-abuse activity.
Source: Threat Hunter original report, page 20

This is a registration tool software for Bilibili captured in June, 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:

息、拼团信息等数据进行爬取。以“拼多多精灵”为例，该工具软件通过请求 piv4.yangkeduo.com 下的接口来爬取拼多多数据， 提供开团提醒、关键词排名、类目排名、导出订单、物流监控、退款提醒、竞品对手监控等功能：

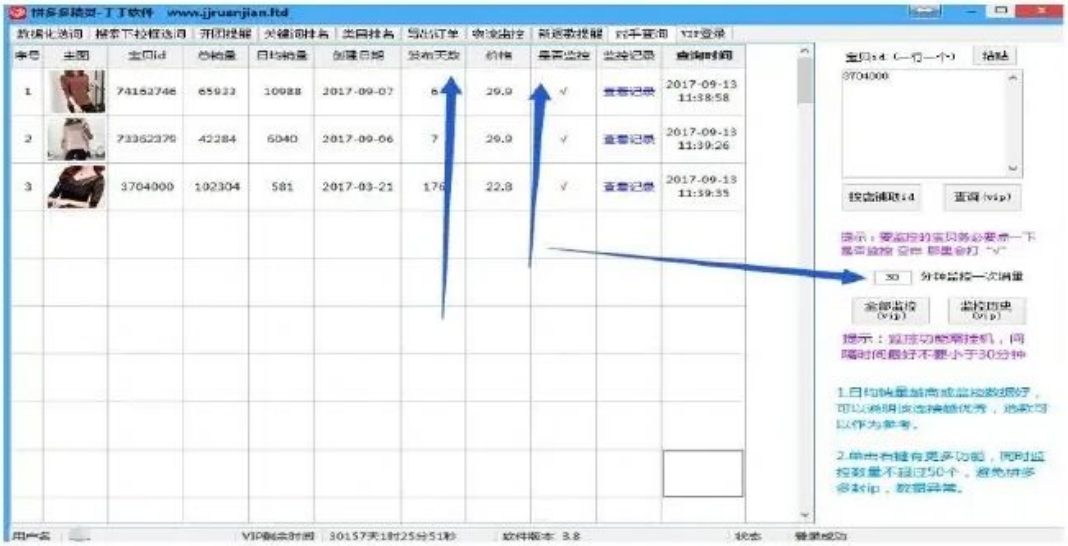


图 3-2-3 拼多多精灵截图 1

Content Climber Tool Software (Chart 1)

Source: Threat Hunter original report, page 21

Content Climber Tool Software (Chart 2)

Source: Threat Hunter original report, page 21

Figure 4-1-1 The running interface of the mobile registration machine of Station B. 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 registration interface of Station B: https://passport.bilibili.com/register/phone and the verification code delivery interface: https://passport.bilibili.com/captcha to extract the verification code, as shown below:

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.

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

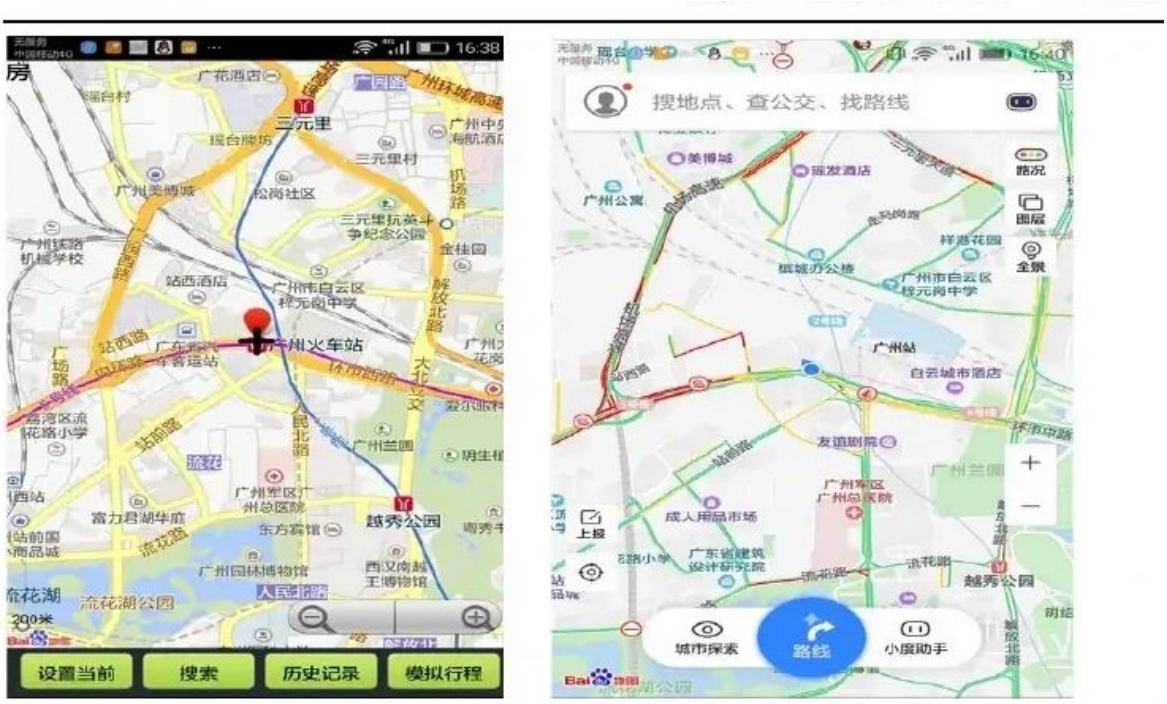


图 3-5-1　　图 3-5-2

Tool software for specific functional categories

Source: Threat Hunter original report, page 23

4.2. Momo red envelope grabbing tool

This is a red envelope-grabbing tool software for Momo captured in July, based on the Android version of Button Wizard. 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 Momo red envelope grabbing tool running interface

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

用接码平台手机号接收手机验证码，同时内置深度学习框架 Caffe 识别图像验证码，

完成帐号批量注册。 程序运行界面如下图：

图 4-1-1 B站手机注册机运行界面

Site B mobile register 3.0

Source: Threat Hunter original report, page 24

Figure 4-2-2 Button Wizard Android version 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 4-2-3 Button Wizard Android version running interface

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 Momo’s 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.

4.3.58 Full-time VIP posting software

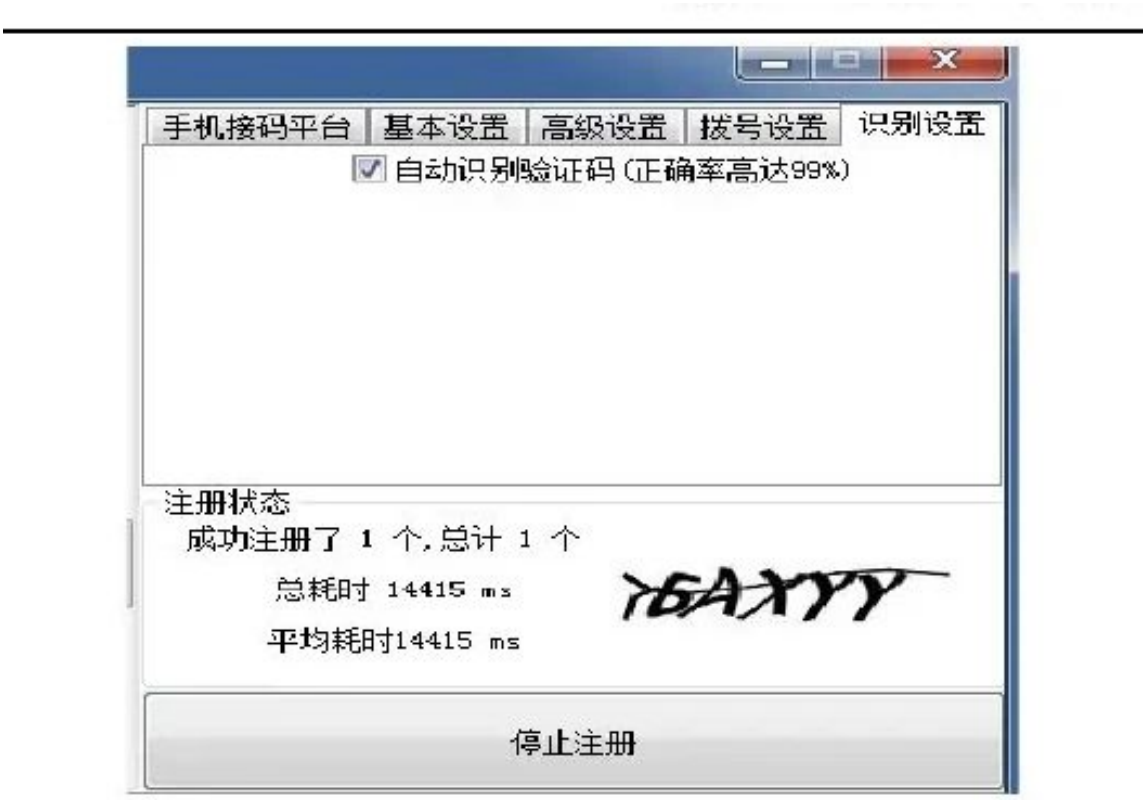


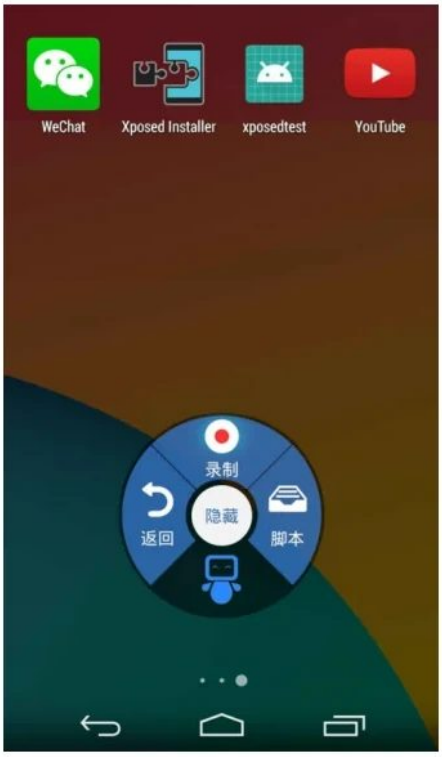
图 4-1-3 深度学习运用于验证码识别

Stranger Red Packer

Source: Threat Hunter original report, page 26

This is an automatic posting tool software for the 58 city captured in August. The principle of this tool is to crack the 58 posting related interface. 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:

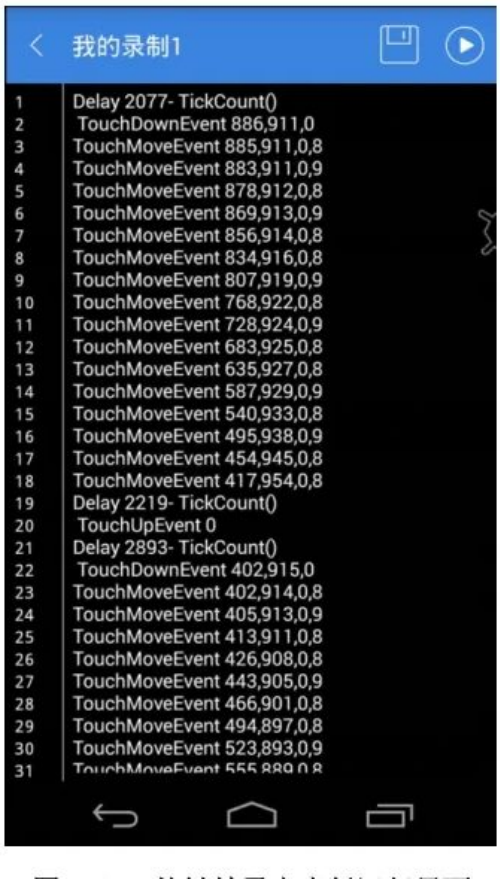
的功能，按键精灵安卓版运行界面如下



Mobile automation tool running interface (Chart 1)

Source: Threat Hunter original report, page 27

Figure 4-3-1 58 full-time VIP posting software running interface There will be many posting-related settings on the interface. These settings were extracted by cybercrime ecosystem staff after analyzing the 58 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:



Tool records touch coordinate, action sequence and delay for automatic replaying of user operations.

Source: Threat Hunter original report, page 29

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):

Full-time VIP posting software

Source: Threat Hunter original report, page 28

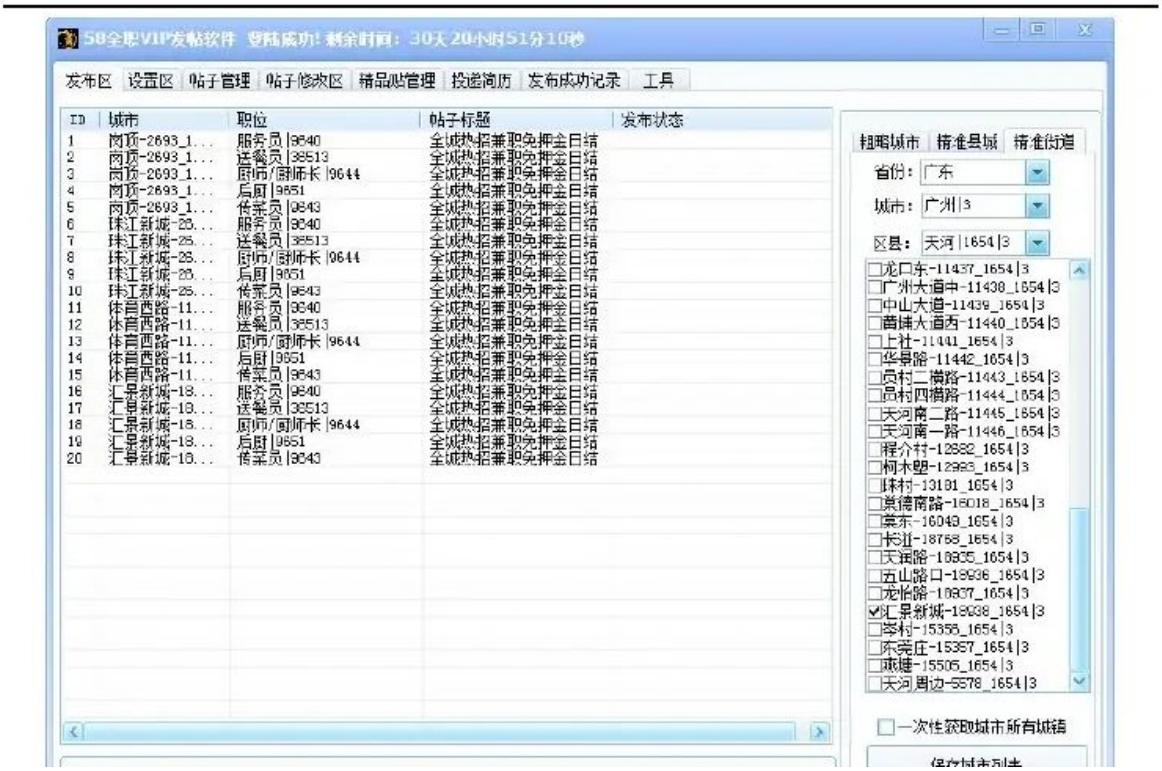
Figure 4-3-3 POST data content (before encoding) We can see that most of the above content is information filled in by users. As long as the same form data is constructed according to the posting interface format, the post can be successfully posted. We can see from the relevant parameters required by 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.

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 up on Taobao's rush buying tools, we found that many users of this tool also use the rush buying tools of JD.com, Suning, Vipshop, Huawei and other 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



Full-time VIP posting software

Source: Threat Hunter original report, page 29