THREAT HUNTER RESEARCH

Online Video Traffic Fraud: Underground Industry Research Report

An investigation into invalid video traffic, the underground services behind it and the signals platforms can use in response.

Original publication: 2019-08-19
Research team: Threat Hunter Research Team
Source report: 30 pages

Original report text

This text version is reconstructed based on the 30-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.

Report statement: This report is exclusively prepared and published by Threat Hunter Guigu Lab. The data involved in the report are taken from the Threat Hunter TH-Karma business intelligence monitoring platform and Internet public data. Limited by data sources, sampling methods, analysis methods and other factors, there may be certain errors between the relevant content in this report and the actual situation.

The copyright of this report belongs to Threat Hunter and is protected by law. Without permission, the text or opinions of the report may not be reproduced, modified or used in other ways. If you need to reprint, please contact Threat Hunter for authorization.

Directory

1. Report Overview

1. 1. Introduction

1. 2. Key points of the report

2. Current status of online video traffic fraud cybercrime ecosystem

2. 1. Overview of the current status of the cybercrime ecosystem

2. 2. Reasons for the existence of cybercrime ecosystem

2. 2.1. The market is eager for quick success, and demand far exceeds supply

2. 2.2. High returns and low risks

2. 3. Overview of the cybercrime ecosystem chain

2. 3.1. Member mode and guest mode

2. 3.2. manipulation price

2. 4. Detailed explanation of traffic manipulation method

2. 4.1. Protocol cracking: high-efficiency and rapid increase in volume

2. 4.2. Group control: Group control upgrade, cybercrime ecosystem operation cost reduction

2. 4.3. Traffic on-hook: Traffic comes from real user IPs across the country

2. 4.4. Multi-open mode: lowest technical threshold

2. 4.5. Manual traffic manipulation: the traffic is real and effective, difficult to detect

2. 5. Comparison of advantages and disadvantages of manipulate mode

2. 6. Flushing characteristics and anti-fraud strategies

3. Analysis of cybercriminal groups that defraud online video traffic

3. 1. traffic manipulation cybercrime operators group data

3. 1.1. Size

3. 1.2. Age level

3. 1.3. Geographical distribution

3. 2. Mostly studio format

3. 3. Diversification of business types

3. 4. Rapid technological updates

3. 5. Wandering in the gray area

4. Write at the end

1. Report Overview

1.1. Introduction

Whether a film or television drama is popular or not, ratings and playback volume seem to be the most intuitive indicators. Too many online videos, whether popular or not, can easily exceed 100 million views. Film and television teams frequently publish promotional releases that exceed 100 million or even 10 billion, which seems to indicate that the playback volume of online film and television dramas has entered the era of 10 billion.

Behind the booming development of the online video and film industry, it is worth pondering whether the beautiful data is true or false, and what kind of negative impact false data can have.

For video platforms, the most direct impact of traffic manipulation is the loss of content copyright distribution and paid value-added service funds.

Secondly, the online video industry is gradually transforming from a traditional free model to a user-paid model. Only by introducing high-quality content and building brand reputation can we seize the position of paying members. However, behind the false data, it directly interferes with the introduction of high-quality content by the platform, affects the user experience and leads to the loss of paying users of the platform.

For advertisers, the falsification of broadcast volume will cause the IP valuation to deviate from the actual situation. The project evaluation of advertisers and investors will be watered down. Not only will the loss of advertising funds fail to achieve the expected conversion effect, but in the long run it will inevitably lead to distortion of the business model and unhealthy market.

For the producers, they appear to be the beneficiaries, but this is not the case. Even if they achieve dazzling performance for a while, it is nothing more than a kind of self-comfort and anesthesia. When producers don’t know which type of content is really liked by users, it will bring a vicious circle to the entire film and television industry.

It is undeniable that false playback of online videos has become a pain point for the entire industry.

The key research object of this report is the online video (long video) online cybercrime ecosystem. The cybercrime ecosystem related to short videos, live broadcasts and other video formats are not within the focus of this report. This report is based on Threat Hunter's threat actors big data. It hopes to reflect the current status of online video traffic fraud with objective and detailed data, and deeply explore the fraud network hidden behind it. It elaborates and analyzes from multiple dimensions such as division of labor content and model, traffic manipulation costs and benefits, traffic manipulation methods and methods, gang characteristics, etc.

1.2. Report key points

- manipulate traffic is mainly active on top online video platforms. From the perspective of manipulate traffic proportion, the top three are Platform A (34.11%), Platform B (27.41%) and Platform C (18.55%).
- Judging from the data of video categories targeted by traffic manipulation, TV series have a large number of episodes and a large total number of traffic-manipulated videos, so they account for the largest proportion of traffic-manipulated videos, reaching 72.69%; for movies, the focus is more on increasing the exposure of the movie by traffic manipulation the playback of trailers, promotional videos or trailers before and after the release, rather than directly increasing the playback of the movie.
- From the perspective of manipulate traffic source IP, more than 99.95% of the traffic originates from domestic IP, covering various provinces, municipalities and autonomous regions in the country, but there is an obvious tendency of geographical aggregation, with the number of IPs belonging to Jiangsu Province and Beijing City exceeding 50%. About 1/4 of the video traffic source IPs belong to IDC computer rooms in various places, and most of them are hosts on major domestic cloud providers.
- Research speculates that there are currently hundreds of thousands of cybercrime operators engaged in online video traffic manipulation, with an annual output value of billions of yuan. The amount of fraud practitioners are mainly concentrated in the post-90s generation, accounting for more than 60%, and they are concentrated in the eastern region of China. Most of the video traffic manipulation personnel exist in the form of studios, with many types of business, rapid technological updates, and various video traffic manipulation methods with different characteristics, each with its own advantages and disadvantages. The popularity of data falsification has shifted from falsifying TV ratings in the early days to falsifying online video playback volume. At present, the popularity of online video falsification is also shifting to the short video and live broadcast industries.
- There are already online video platforms that have taken the lead and continued to actively fight against the cybercrime ecosystem, and the effect is remarkable. However, the active confrontation of a few platforms cannot severely damage the entire cybercrime ecosystem, and the entire industry needs to work together to combat it.

2. Online video traffic fraud cybercrime ecosystem status quo

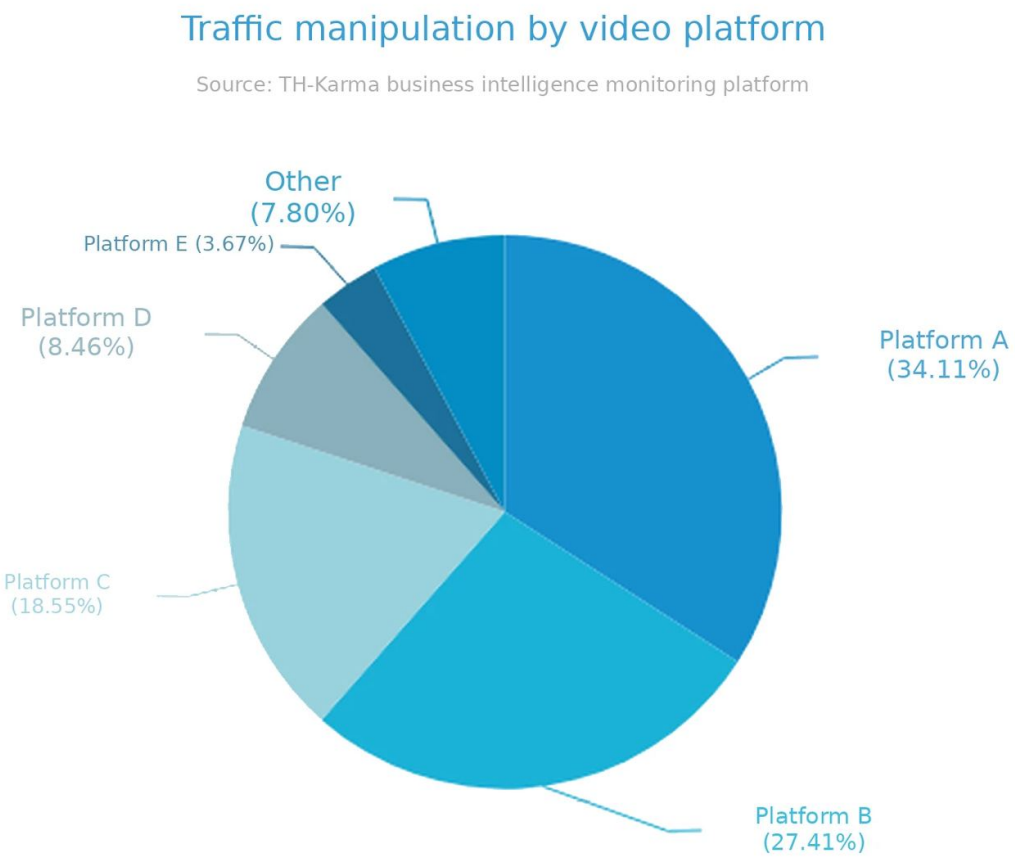
2.1. Overview of the current status of the cybercrime ecosystem

iResearch predicts that the market size of China's online video industry is expected to reach 212.97 billion yuan in 2020, with an expected compound annual growth rate of 34.98% from 2016 to 2020. The huge industry market value not only attracts many video content creators to join in, but also attracts the attention of cybercrime actors. In addition, the legal and regulatory systems have yet to be improved, and the crime costs of video traffic manipulation are low and the returns are high in a short period of time, attracting a large number of people to invest in the cybercrime ecosystem of video traffic manipulation. Research speculates that there are currently hundreds of thousands of cybercrime operators engaged in video traffic manipulation, with an annual output worth billions of yuan.

Although a few video platforms have actively fought against fake playbacks, such as one leading platform, which has strengthened anti-swiping measures and announced that it will close the

front-end playback display, challenging the "only playbacks" theory, which has reduced playback fraud to a certain extent, it has not had a great impact on the entire cybercrime ecosystem.

Judging from the long-term video traffic manipulation data captured by the Threat Hunter TH-Karma business intelligence monitoring platform, the platforms targeted by traffic manipulation are mainly concentrated in leading platforms that have occupied a large market share, such as Platforms A to E, as shown in the following figure:



Share of manipulated traffic by video platform: the five leading platforms account for more than 90%

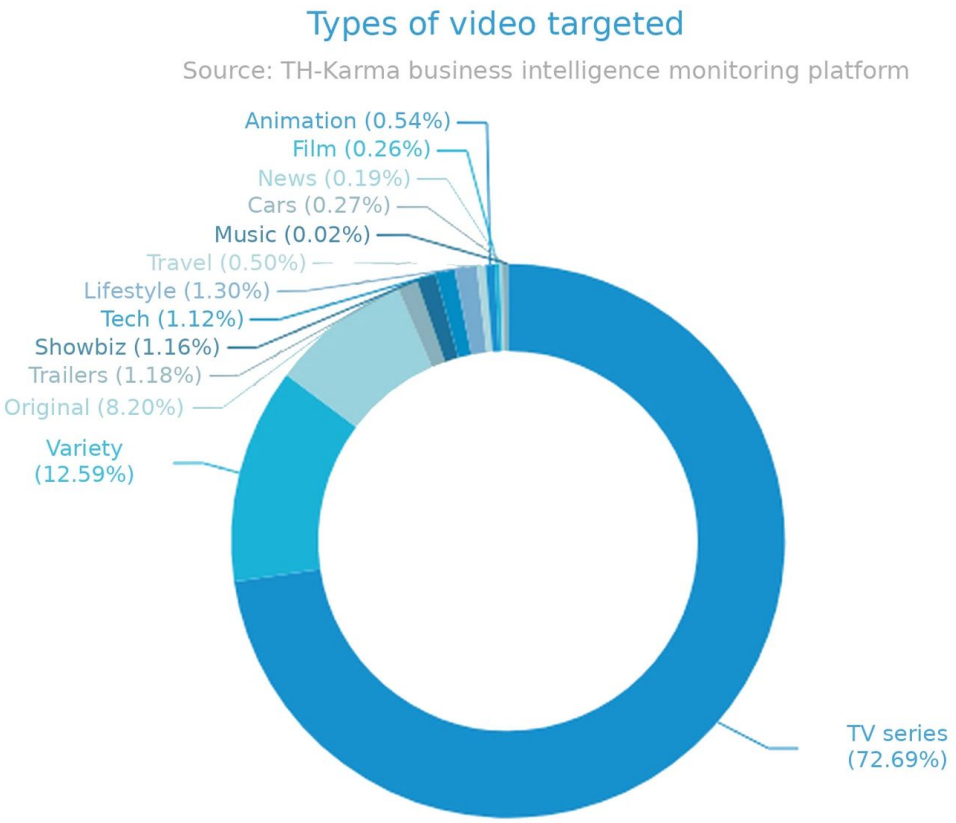
Source: Threat Hunter original report, page 6. Original figure with Chinese text replaced by English.

The reason is that the video sharing mechanism of these top platforms is more complete, and manipulating traffic volumes can not only obtain more video sharing, but also achieve better promotion effects.

Judging from the data of video categories targeted by traffic manipulation, TV series have a large number of episodes and a large total number of traffic-manipulated videos, so they account for the largest proportion of traffic-manipulated videos, reaching

72.69%; For movies, it focuses more on increasing the number of views of trailers, promotional videos or trailers before and after the release.

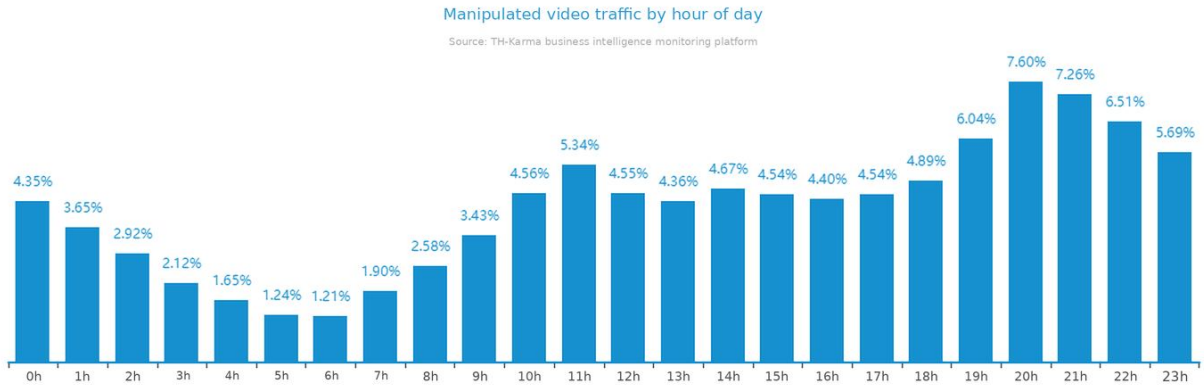
The exposure of the movie, rather than the playback of the movie directly, see the figure below for details:



Types of video targeted: TV series account for 72.69% of manipulated traffic

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

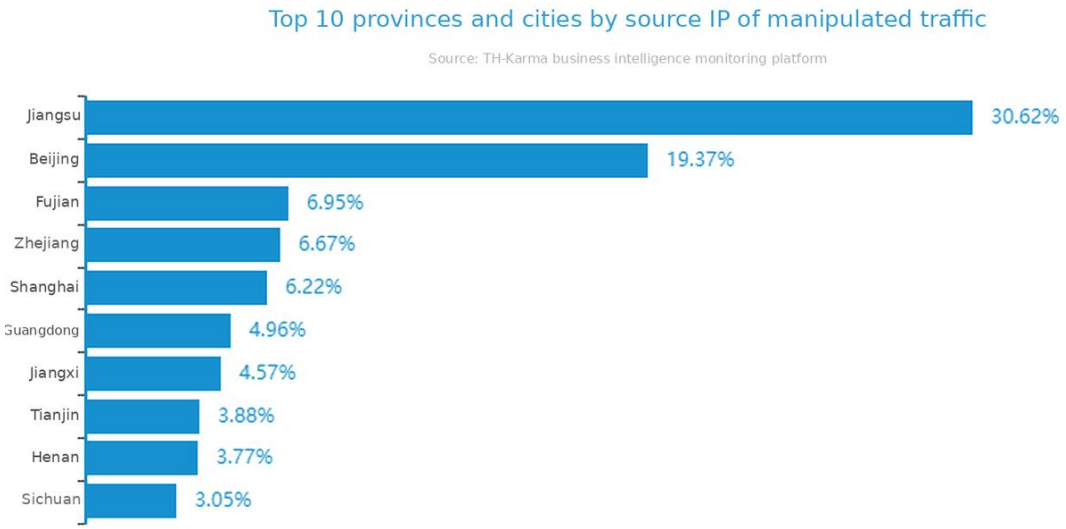
cybercriminal groups attack behavior will imitate the behavior of real users to increase the difficulty for companies to identify abnormal traffic. Whether it is video cybercrime ecosystem, advertising click fraud, article reading fraud, etc., the traffic will be as consistent as possible with the access habits of real users. The figure below shows the time distribution of video traffic manipulation traffic within 24 hours. The peak period of traffic manipulation is from 19:00 to 23:00 at night, and reaches the highest value at 20:00 during prime time:



Manipulated video traffic by hour: it follows normal viewing times and peaks in the evening

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

Analyzing from the perspective of video traffic source IP, more than 99.95% of the traffic originates from domestic IPs, covering various domestic provinces, municipalities and autonomous regions, but there is obvious geographical aggregation. Among the source IPs of video traffic, the number of IPs belonging to Jiangsu Province and Beijing City exceeds 50%. About 1/4 of the video traffic source IPs belong to IDC computer rooms in various places, and most of them are hosts on major domestic cloud providers. The statistics of the top ten provinces and cities where video traffic manipulation source IP belongs are shown in the figure below:



Top 10 provinces and cities by source IP of manipulated traffic, led by Jiangsu

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

In addition, Threat Hunter recently detected that the TV series "Wind Knife", which was launched on a certain video platform on December 27, 2018 and starred a number of popular traffic niche actors, had hundreds of millions of false views within one month of its launch; the Thai movie "The Means of Surrendering to Sex" was released on January 16, 2019. It was released on the same day, and a Thai subtitle group, as the driving force behind the scenarios, wanted to increase the exposure of the film by creating tens of millions of false views of the promotional video every day.

2.2. Reasons why the cybercrime ecosystem exists

2.2.1. The market is eager for quick success, and demand far exceeds supply.

There are many interests involved behind the false playback volume of online videos, which is far greater than the supply demand. This is the main reason why fraud in video playback volume is repeatedly prohibited. The online video industry mainly involves three major roles: video platforms, advertising investors, and producers.

The producer is the party with the greatest demand for video playback. The most intuitive purpose is to get more traffic and video sharing from video websites. High playback volume can improve rankings, attract more users to watch, and naturally gain more traffic. For video sharing, it mainly includes advertising period sharing, content sharing, and member payment period sharing, and the effective playback volume is an important indicator of settlement.

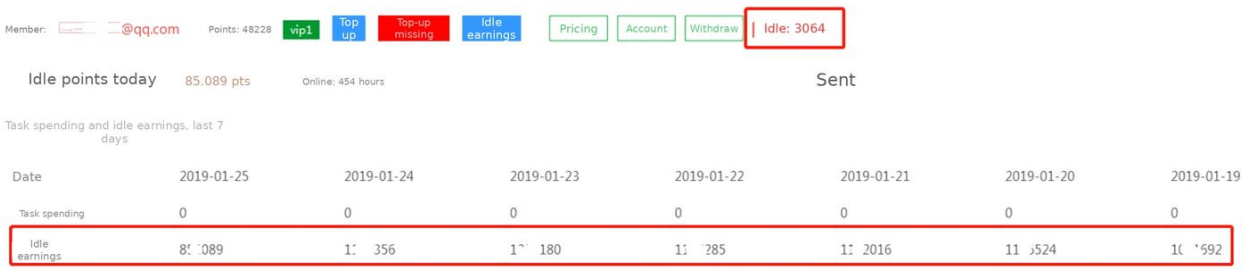
Secondly, some film studios have signed gambling agreements with advertisers, and traffic manipulation up the volume can not only avoid the risk of gambling failure, but also inflated data is an important capital for subsequent investment.

Nowadays, when IP is king, the amount of traffic can not only help the film producers create a "hit" film and television drama, or win over directors and stars, but the traffic of high-profile IP can also bring huge added value and resources.

traffic manipulation volume can be said to be the simplest and most effective gold-raising method. For those who don’t have big-name stars or a strong team, in many cases the producers of online movies don’t even have the manpower and material resources for publicity. Compared with other expensive marketing and promotion plans, a few to dozens of yuan for 10,000 visits can be said to be simple and efficient, but the value of click sharing or pre-roll advertising in exchange is far higher. Under this model of quick success and instant benefit, it is not difficult to understand why the phenomenon of volume traffic manipulation continues to be banned.

2.2.2. High return and low risk

In the process of our investigation and research, we came into contact with user A of a P2P online traffic manipulation platform. User A told us how he earned thousands of yuan a day by logging on to increase his trading volume. User A told us that he has deployed more than 3,000 idle clients on a large number of machines, earning an average of more than one million points per day. Although the platform does not support the direct withdrawal of idle points, it can be indirectly cashed out by transferring points to other users. According to the platform's rule of recharging 10 yuan = 10,000 points, user A can indeed earn a thousand yuan a day easily. The picture below shows the recent AFK points income shown to us by User A (for details on AFK traffic manipulation, please see Section 2.4.3):



An idle-client user's earnings page: points earned, hours online and the last seven days of activity

Source: Threat Hunter original report, page 10. Original figure with Chinese text replaced by English.

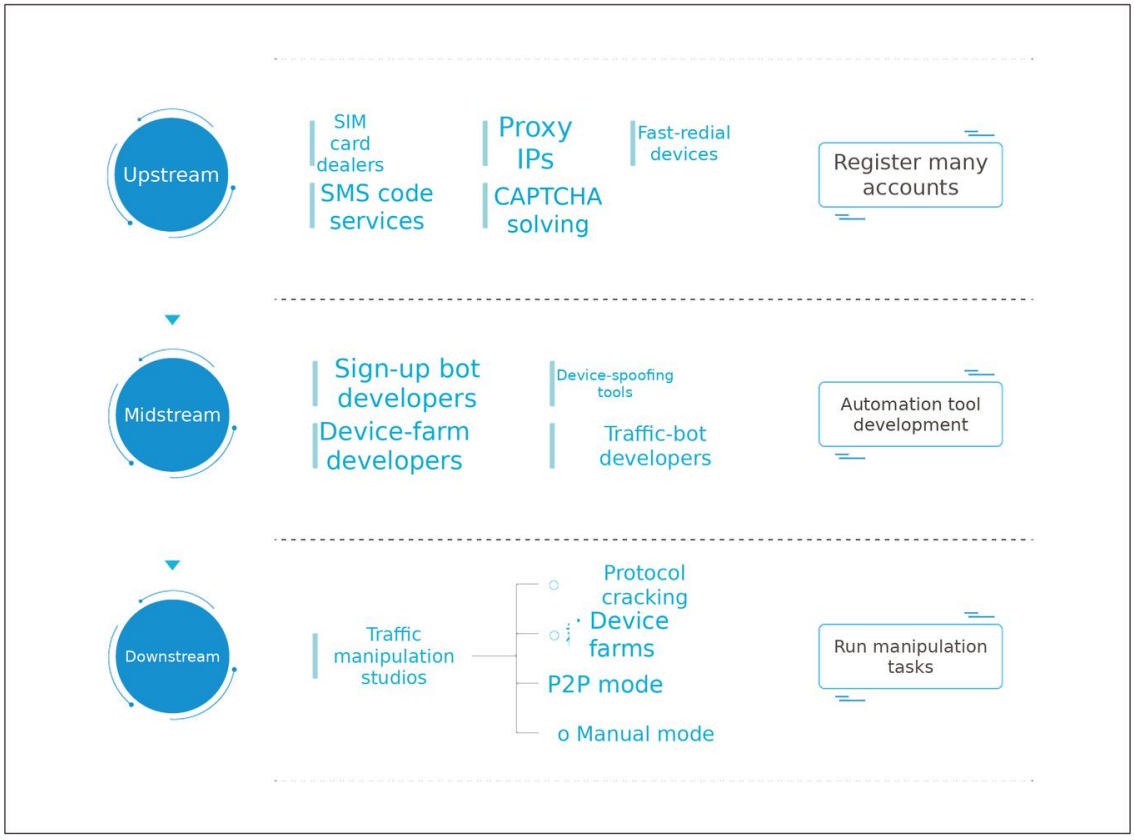
User A is just a small microcosm of the huge army of manipulate washers. For manipulate wash practitioners, if they dare to take risks and wash their hands, on the one hand, they can quickly obtain huge profits, and on the other hand, the cost of breaking the law is low. Every link in this industry chain is basically huge profits. The monthly income of upstream card dealers exceeds 100,000 or even millions. The volume-burning studios claim to be able to generate at least tens of millions of views every day, and the illegal profits are also very considerable. However, the current laws against video traffic manipulation are not perfect. In the first domestic prosecution case against traffic manipulation, a traffic manipulation company caused at least 950 million false visits to a leading video platform. The company also undertook the traffic manipulation business of other mainstream video platforms. It was conservatively estimated that the illegal profit was more than one million, but in the end it was only awarded 500,000 in compensation.

2.3. Overview of the cybercrime ecosystem chain

2.3.1. Member mode and guest mode

Currently, the mainstream video playback modes are divided into two modes, one is member login playback, and the other is guest mode. The two playback modes have also given rise to two different traffic manipulation industry chains with clear division of labor.

For the membership model traffic manipulation industry chain, the entire industry chain can be divided into three major modules: upstream, midstream, and downstream as shown in the figure below:



The traffic manipulation chain in member mode: upstream resources, midstream tools and downstream studios

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

To complete the video volume increase in the membership model, you must first register a large number of platform accounts. A detailed analysis of the upstream account registration process is as follows:

(1) Roles and Resources a) Card dealers: Under the guise of normal business, they obtain mobile phone card resources from operators or agents through various channels, and then sell them to downstream card dealers, SMS verification-code receiving services, and downstream number dealers at a markup to earn the price difference. The mobile phone cards it provides can be divided into: virtual card/real card, voice card/text message card, foreign card/Chinese mainland card, data card/registered card.

b) SMS verification-code receiving service: Responsible for connecting card merchants and groups with mobile phone verification code needs, providing software support, business settlement and other platform services, and profiting from business sharing.

c) CAPTCHA-solving service: a platform mainly used to identify image verification codes. When registering a video website account, various forms of verification codes are generally used to prevent batch registration of machines. CAPTCHA-solving services can break this restriction. The CAPTCHA-solving service can use software machines to code, or it can recruit "coders" to do the coding manually.

d) Proxy IP: The proxy IP platform provides a large number of proxy IP resources. Using proxy IP as a springboard, you can hide your real IP. By constantly switching IPs, the fraud-control strategy of the video platform in the IP dimension can be bypassed.

e) Second dial machine: Second dial machine can be understood as a dial-up VPS, that is, a dynamic dial-up virtual machine, which can switch IP through broadband dial-up.

Compared with proxy IP, the IP dialed by the instant dialer is a real broadband dial-up IP, which is more difficult to detect and prevent for video platforms.

(2) Cost and profit analysis a) Card dealer: Depending on the type of mobile phone card, the price of each mobile phone card is different. The average price of some card types is as follows:

Prices of SIM cards used for bulk sign-ups

SIM card type	Virtual-operator numbers: wholesale	Virtual-operator numbers: retail	Major-carrier numbers: SMS only	Major-carrier numbers: with voice	Real-name SIM
Price (CNY per card)	5	10	14	20	100

Prices of SIM cards used for bulk sign-ups vary with operator, function and real-name status

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

The card dealer connects the illicit SIM card to the SMS verification-code receiving service and provides the service of accepting mobile phone verification codes. Depending on the registration project, each mobile phone verification code can earn income ranging from 0.01 yuan to 3 yuan.

b) SMS verification-code receiving service: In addition to the platform’s own profit from the mobile phone card receiving code, the other part of the income is the income share of the access card provider from sending and receiving verification codes, which is generally about 30%.

c) CAPTCHA-solving service: Coding prices vary according to the type of verification code and its complexity. The following is an example of the price of a CAPTCHA-solving service:

Prices for solving CAPTCHAs

CAPTCHA type	4 digits	4 letters	4 letters and digits	4 Chinese characters	Arithmetic
Price (CNY per CAPTCHA)	0.01	0.01	0.01	0.04	0.014

Prices for solving CAPTCHAs depend on the character type and complexity

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

traffic manipulation studios will purchase registration machine tools for batch registration of leading video platforms from software developers, and combine the CAPTCHA-solving service and

CAPTCHA-solving service to quickly register platform accounts in batches. Some studios will also directly purchase a large number of platform membership accounts from account providers. Finally, the video can be played, liked, commented and other operations through protocol cracking traffic manipulation tools, group control or manual traffic manipulation.

The biggest difference between the guest mode traffic manipulation industry chain and the membership model industry chain is that there is no need to log in to complete the video traffic manipulation. In guest mode, for cybercriminal groups, the account cost during the traffic manipulation process is reduced, but for video platforms

For the platform, the lack of user ID as a detection dimension makes it more difficult to detect traffic manipulation behavior. Through the investigation and analysis of the traffic manipulation gangs, the visitor mode is the current mainstream traffic manipulation mode. Please see Section 2.4 for details of the traffic manipulation methods.

2.3.2. manipulation price

The price of traffic manipulation is related to the size of the platform and the platform's fraud-control rules. We combine the quotations of different traffic manipulation groups and calculate the average price of traffic manipulation on each major video platform, as follows:

Traffic manipulation prices by video site

Site	Plays (CNY per 10,000)	Subscribers (CNY per 10,000)	Likes / dislikes (CNY per 10,000)	Comments (CNY each)	Bullet comments (CNY each)
Youku	4	110	70	0.4	0.9
iQiyi	50	280	70	0.4	0.9
Tencent Video	4	800	/	1.4	0.7
bilibili	230	1,600	/	1.4	0.9
Sohu Video	50	400	120	0.4	0.7
AcFun	2	/	200	/	/
PP Video	11	/	/	/	/
LeTV	3	/	130	/	/
Mango TV	2	/	/	/	/
Wasu	2	/	/	/	/

Traffic manipulation prices differ widely across video sites and services

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

The traffic manipulation business and traffic manipulation price will be adjusted as the platform's fraud controls intensity and effectiveness change, and are highly time-sensitive. For example, in July 2018, a leading video platform strengthened anti-traffic manipulation measures, and some traffic manipulation gangs temporarily suspended related businesses until a seller claimed to have exclusive non-dropping technology, but the traffic manipulation price rose sharply to 100 yuan/10,000 times. On September 3, 2018, after the same platform announced that it would close the front-end playback display, many studios stated that they would no longer undertake related business.

2.4. Detailed explanation of traffic manipulation method

2.4.1. Protocol Cracking: Efficient and Rapid Volume Uploading

Protocol cracking, that is, cybercrime ecosystem cracks the communication protocols and algorithms in the communication between the client and the server, and forges corresponding requests and parameters to directly access the communication interface to achieve the purpose of traffic manipulation.

Take the latest version of the tool called "Dianlong Video Flashing Software" that we captured in April 2018 as an example. It supports:

```
.rdata:0051AD0D                 db 'User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:27.0) Gecko/20'
.rdata:0051AD0D                 db '100101 Firefox/27.0',0Dh,0Ah
.rdata:0051AD0D                 db 'Connection: Keep-Alive',0Dh,0Ah
.rdata:0051AD0D                 db 'Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3',0Dh,0Ah
.rdata:0051AD0D                 db 'Accept-Encoding: deflate',0
.rdata:0051ADEB aVid_0          db   'uid',0              ; DATA XREF: sub_411F3A+7C↑o
.rdata:0051ADEB                                           ; sub_419498+189↑o
.rdata:0051ADF1 aInvoker1Callba db '&invoker=1&callback=playerBack',0
.rdata:0051ADF1                                           ; DATA XREF: sub_411F3A+13E↑o
.rdata:0051AE10 aCid            db '&cid=',0              ; DATA XREF: sub_411F3A+146↑o
.rdata:0051AE16 aHttpVc_mgtv_co db 'http://vc.mgtv.com/v2/watch?&pid=&vid=',0
.rdata:0051AE16                                           ; DATA XREF: sub_411F3A+14E↑o
.rdata:0051AE3D aHostVc_mgtv_co db 'Host: vc.mgtv.com',0Dh,0Ah ; DATA XREF: sub_411F3A+20A↑o
.rdata:0051AE3D                 db 'Accept: */*',0Dh,0Ah
.rdata:0051AE3D                 db 'User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:27.0) Gecko/20'
.rdata:0051AE3D                 db '100101 Firefox/27.0',0Dh,0Ah
.rdata:0051AE3D                 db 'Connection: Keep-Alive',0Dh,0Ah
.rdata:0051AE3D                 db 'Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3',0Dh,0Ah
.rdata:0051AE3D                 db 'Accept-Encoding: deflate',0
.rdata:0051AF1A aCode0          db '"code":0',0           ; DATA XREF: sub_411F3A+359↑o
.rdata:0051AF22 aVideoid2       db 'videoid2',0           ; DATA XREF: sub_41232C+99↑o
.rdata:0051AF2B aId1            db   video id1',0         ; DATA XREF: sub_41232C+118↑o
.rdata:0051AF33 a1512108        db '1512108',0            ; DATA XREF: sub_41232C+1D9↑o
.rdata:0051AF3B a369c147be259c0 db '369C147BE259C037',0   ; DATA XREF: sub_41232C+1E1↑o
.rdata:0051AF4C a58             db '58',0                 ; DATA XREF: sub_41232C+1E9↑o
.rdata:0051AF4F a152pfqejiRvpvi db '152PFQejI&rvpvid=&ycid=&rycid=&r_=',0
```

Disassembled code of a protocol-cracking tool builds request parameters that imitate the client

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

The traffic manipulation of multiple leading video platforms. As shown below, the URL and HTTP request header constructed within the software for one of these platforms:

In order to avoid multiple accesses from a single IP, such tools also have built-in dial-up functions and proxy IP website interfaces. As shown in the figure below, this tool can obtain proxy IPs in batches through the built-in proxy interface, so this traffic manipulation behavior cannot be identified from the IP dimension alone:

```
.method public static hidebysig string GetIpRes(string _orderNo, string _secret, string _url)
                                        // CODE XREF: ZD_Demo.Program__Main+78↑p
{
  .maxstack 5
  .locals init (string V0)
  ldstr     aForward_xdaili           // "forward.xdaili.cn"
  stloc.0
  newobj    instance void [System]System.Net.WebClient::.ctor()
  dup
  callvirt instance class [System]System.Net.WebHeaderCollection [System]System.Net.WebClient::get_Headers()
  ldstr     aProxyAuthoriza           // "Proxy-Authorization"
  ldarg.0
  ldarg.1
  call      string ZD_Demo.ZDHelper::authHeader(string orderno, string secret)
  callvirt instance void [System]System.Collections.Specialized.NameValueCollection::Add(string, string)
  dup
  ldloc.0
  ldc.i4.s 0x50
  newobj    instance void [System]System.Net.WebProxy::.ctor(string, int32)
  callvirt instance void [System]System.Net.WebClient::set_Proxy(class [System]System.Net.IWebProxy)
  ldarg.2
  callvirt instance string [System]System.Net.WebClient::DownloadString(string)
  ret
}
```

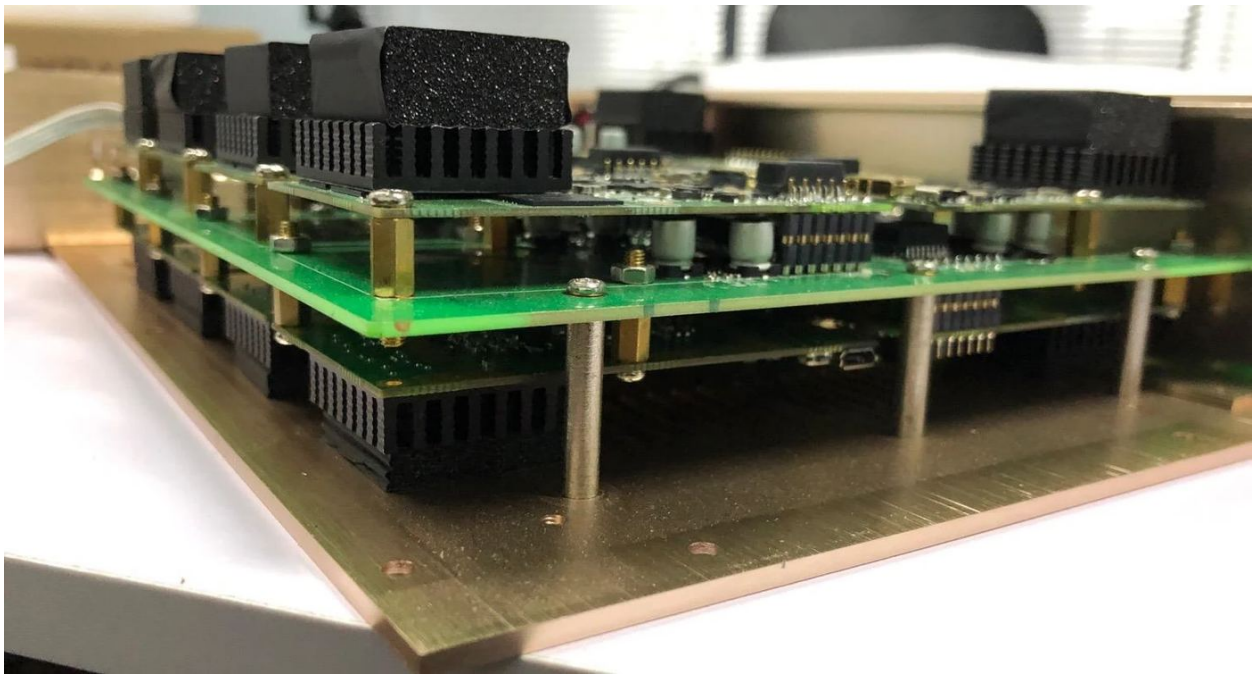
The tool sends requests through proxy IPs to avoid repeated access from one IP

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

This type of tool mainly makes money by users purchasing card codes and recharging. However, because the tool can be obtained externally, its core logic can be analyzed through reverse debugging. At the same time, some people have cracked it and released a free version. As a result, this type of tool is basically no longer sold to the outside world. Tools such as "Tianlong Video traffic manipulation Software" have been acquired by manipulate Studio and used as internal tools.

2.4.2. Group control: Group control upgrade, cybercrime ecosystem operation cost reduction

Now many cybercrime ecosystem studios are using a new type of group control, which we call box group control. Box-type group control is an upgraded variant of traditional group control. Compared with traditional group control, box-type group control no longer requires external mobile phone equipment. Instead, multiple mobile phone chips are directly packaged in a chassis, and the mobile phone screen is displayed on the client installed on the control computer through the network. This reduces the cost of mobile phone batteries, screens and other hardware, and saves space. The size of box-type group control is only one-quarter of an ordinary desktop computer chassis. The following figure shows the internal structure of the box-type group control:



Box-based device farm hardware: many phone boards controlled by one computer

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

Box-type group control software and hardware are sold in complete sets. Box-type group control software is significantly better than traditional group control software in terms of stability, software and hardware compatibility, and functional perfection. By virtually dividing the memory of the mobile phone chip, multiple devices can be opened. Each mobile phone chip can be split into ten "mobile phones". Different device information can be forged for each "multiple mobile phone", such as IMEI, mobile phone location, local number, network information, etc. You can also install apps in batches, set proxy IPs, and modify mobile phone device information through computer client operations. A comparison of the advantages and disadvantages of box-type group control and traditional group control is as follows:

In short, box-type group control greatly reduces the manual operating costs of cybercrime ecosystem studios, and at the same time solves the problems of traditional group control configurations, complicated operations, and battery consumption of mobile phones.

Box-based versus traditional device farms

Item	Box-based device farm	Traditional device farm
Hardware and software compatibility	Strong	Weak
Configuration complexity	Low	High
External phones needed	No	Yes
Virtual phone cloning	Supported	Not supported
Hardware cost / wear	Low	High
Floor space	Small	Large

Box-based device farms suit large-scale operations better than traditional ones

Source: Threat Hunter original report, page 16. Table re-typeset in English from the original.

The use of group control to traffic manipulation solves to a certain extent the problems of difficult protocol cracking and slow manual traffic manipulation. The general operation process of batch registration and traffic manipulation using automated scripts is as follows:

(1) Register accounts on multiple mobile phones at the same time:

- Use the modification software to forge the fingerprint of the device, then open the App and click to register;
- Call the SMS verification-code receiving service API, receive and enter the phone number, click to receive the verification code, wait for the SMS verification-code receiving service to return the verification code and enter it to complete the registration;
- Record the account number, password and device information of the modification tool into a text file, and return to the first step for the next round of registration.

(2) Multiple mobile phones manipulation data at the same time:

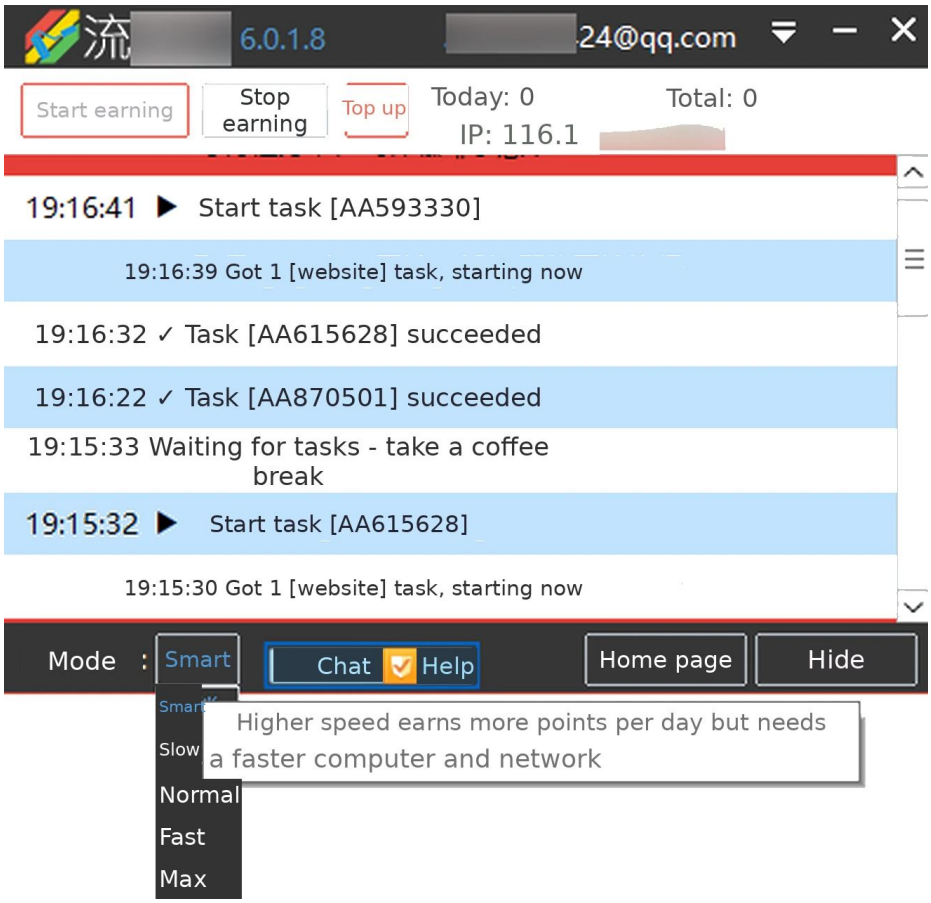
- Forge device fingerprints and open the video app (if necessary, you need to log in to your account);
- Search for the video selected for traffic manipulation, open the video, press playback settings to start traffic manipulation, and after completion, return to the first step for the next round of traffic manipulation. Video playback settings include setting the playback duration, setting the volume, whether to play continuously, selecting the definition, automatic refresh and automatic cache clearing, etc.

2.4.3. Traffic hangup: Traffic comes from real user IPs across the country

Traffic AFK is a data fraud model based on the P2P principle to achieve traffic optimization, video traffic manipulation, ranking traffic manipulation and other functions. It is completed by the cooperation of two parts, the AFK user and the traffic demand user.

First, a large number of AFK users download and run the AFK software, fill in the account number or AFK number, and stay online. Based on the AFK time and the number of completed tasks, they can earn platform points and finally realize them. Traffic users are users who need promotion. They can publish tasks on the traffic platform. The server will assign the received task requests to idle users and automatically complete the traffic manipulation task. The traffic data comes from real computer users across the country.

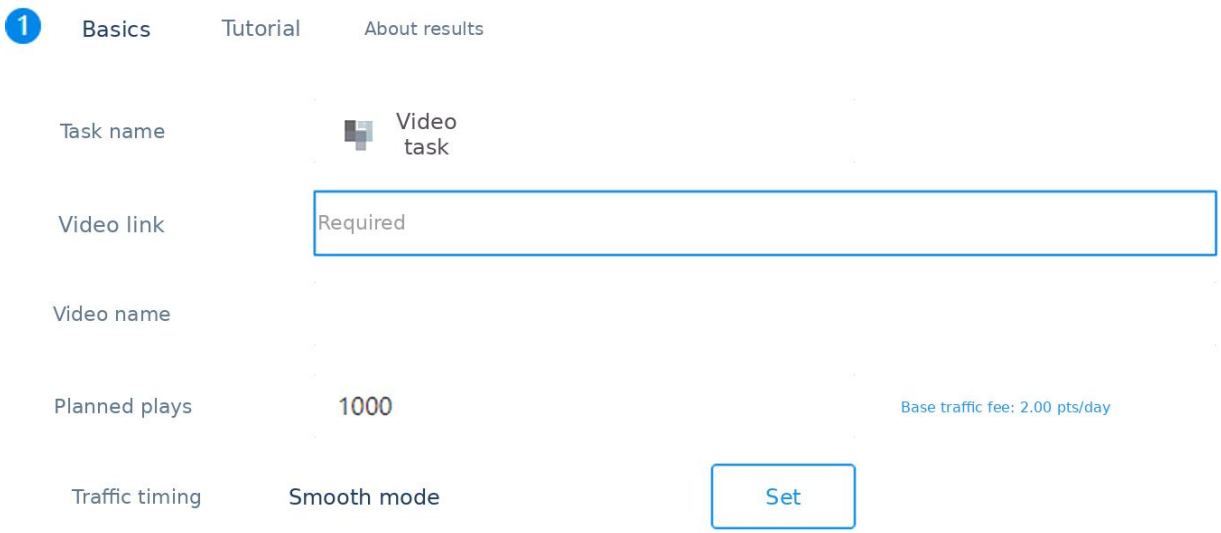
(1) Idle-client users can earn points by remaining connected: The interface of a certain idle-client software is as follows. After downloading and logging in to the idle-client software, select the point earning mode and click Start Earning Points to automatically start to obtain tasks and automatically execute tasks. After the task is successfully executed, corresponding points will be obtained:



The idle-client software takes tasks from the platform and logs each one

Source: Threat Hunter original report, page 17. Original figure with Chinese text replaced by English.

(2) Traffic demand users release tasks: Take a certain traffic tool as an example to introduce the basic settings of task release:



Task settings on the traffic side: video link, planned plays and traffic timing

Source: Threat Hunter original report, page 18. Original figure with Chinese text replaced by English.

- Video link: Fill in the video link address that needs to be optimized for playback volume;

- Video name: After filling in the video link, it will be automatically recognized, no need to fill it in manually;
- Planned playback volume: fill in the daily playback volume of the video selected for traffic manipulation;
- Flow time control: There are two ways, smooth mode and high-speed mode:

 Smooth mode: The system automatically allocates the planned traffic volume between 0 and 23 points. It is generally recommended to default, which is suitable for customers who do not urgently need a large amount of playback in a short period of time;

 High-speed mode: Complete the planned traffic volume set by the user in the shortest time, generally expected to be completed within 1 to 6 hours.

Suitable for users who urgently need to quickly increase playback volume in a short period of time.

- After setting various settings, save the task and click Start to optimize the task immediately.

The picture below shows the video traffic manipulation task setting interface:



Traffic timing: planned visitors are spread across the 24 hours of the day

Source: Threat Hunter original report, page 18. Original figure with Chinese text replaced by English.

(3) Cost and Price For idle-client users, generally a single client can earn a few cents to several yuan by remaining connected for 24 hours. The amount of income earned by remaining connected is related to many factors, including but not limited to computer configuration, network conditions, computer system idle rate, number of tasks issued by the server, type of tasks issued by the server, optimized speed settings on the software, software online time, etc.

For users with traffic demand, the cost of video traffic manipulation varies according to the video platform being traffic-manipulated. In addition to the basic fee for playback volume, additional fees will be charged based on the set IP number, traffic manipulation mode, etc. based on the basic traffic fee. The following are

The following table summarizes the pricing used by an idle-client traffic platform for some video platforms:

Pricing of an idle-client traffic platform

Video platform	Base fee (CNY per 10,000 IPs)
Tencent Video	20
bilibili	20
Mango TV	30
Sohu Video	20
Sina Video	10
NAVER	50
Meipai	10
Douyu Video	40

Value-added fees: IP volume surcharge - above 10,000 IPs, 20% to 100% of the base fee depending on the number of IPs; high-speed mode surcharge - 50% of the base fee.

Pricing of an idle-client traffic platform by video site, plus volume and speed surcharges

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

2.4.4. Multi-open mode: lowest technical threshold

The purpose of manipulating traffic volumes in the multi-open mode is mainly to open multiple video windows to achieve the purpose of manipulating traffic volumes. This mode is relatively low in technical difficulty and cost. There are two main methods: opening multiple browsers and opening multiple simulators.

To watch videos in a browser, you need to clear your browsing history and historical data, then open an incognito window and use Flash player to watch. Currently, UC Browser and 360 Browser are more stable and effective for traffic manipulation. The specific traffic manipulation process is as follows:

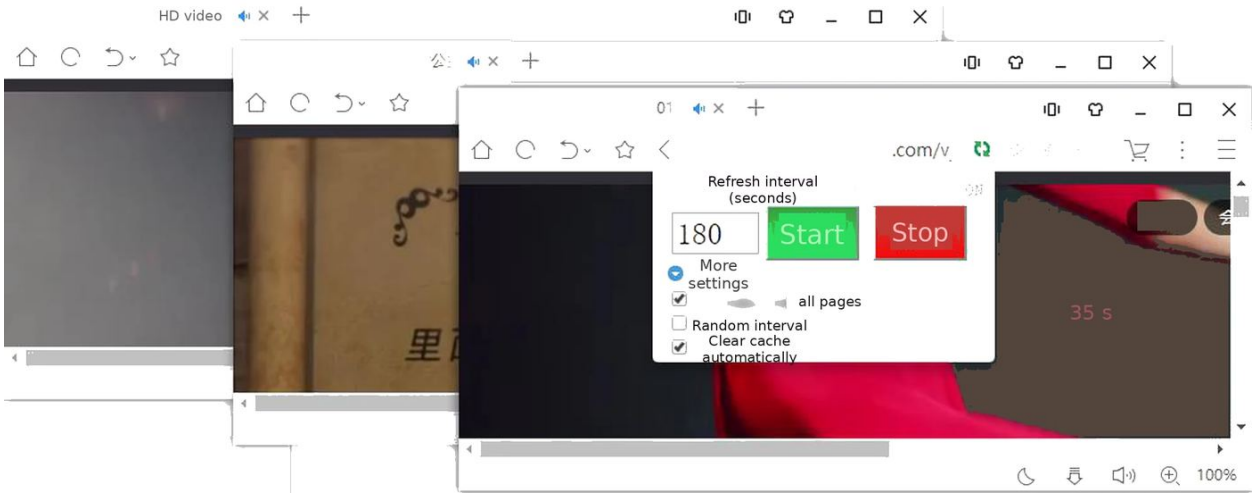
(1) Open the browser and download the automatic refresh plug-in;

(2) Open the video website and search for videos that need to be refreshed;

(3) Set the automatic refresh time, which must be greater than the advertising time, generally 2 to 3 minutes is appropriate;

(4) The automatic refresh plug-in must check [Automatically clear cache], and click Start after successful setting;

(5) The browser can open multiple windows at the same time according to the computer performance. The window needs to be dragged out into an independent window, and the window cannot be minimized;



Multi-window mode: an auto-refresh browser plug-in reloads the video page at set intervals

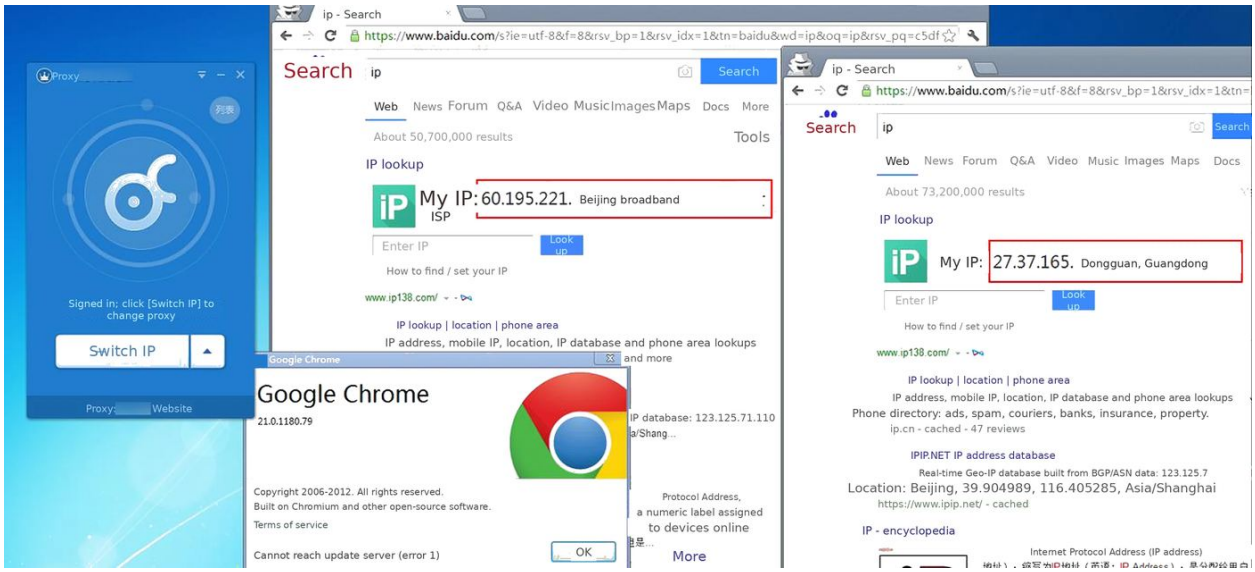
Source: Threat Hunter original report, page 20. Original figure with Chinese text replaced by English.

(6) Video playback cannot be muted.

Open more traffic manipulation through the browser. For traffic manipulation that can be completed without logging in to the video platform member account or using other tools, traffic manipulation can be said to be zero cost. Assuming that the browser is refreshed every 3 minutes and the browser opens 25 more windows, each computer can complete 500 refreshes per hour.

Simulator multi-open is an optimized version of browser multi-open. By forging simulator parameters, combining proxy IP, etc., you can achieve simultaneous traffic manipulation on multiple simulators.

In order to solve the problem of single IP ban, a certain proxy client has an old version of Chrome browser built-in. It can open multiple browsers and assign different proxy IPs to each browser, as shown in the figure below:



A proxy client gives each browser window a different IP to avoid single-IP blocking

Source: Threat Hunter original report, page 20. Original figure with Chinese text replaced by English.

2.4.5. Manual traffic manipulation: the traffic is real and effective and difficult to detect

When encountering a video traffic manipulation task with specific requirements or the traffic manipulation is very difficult, it can be completed through manual traffic manipulation. Manual traffic manipulation is divided into paid task dispatch and free platform mutual traffic manipulation.

Distributing orders for traffic manipulation tasks refers to gathering real users through various channels such as instant-messaging groups and online forums, and using their own accounts to send orders to specific users.

For videos to be watched, liked, commented on, etc., one link per member is counted as one playback volume. According to the number of links, you can get cash rewards ranging from 0.1 to 0.5 yuan per link.

Mutual promotion on the platform is to share video links that need to be boosted in the mutual aid group. Group members click on each other as required, and are generally required to watch the entire video.

The manual traffic manipulation mode is completely performed by real users and is technically impossible to detect. The method is simple and there are no technical barriers. However, the cost of traffic manipulation is relatively high. Judging from the currently monitored intelligence, this type of mode is not widely used in video traffic manipulation. There are also studios that claim that their traffic manipulation method is purely manual, but the quotation given is far lower than the cost. This may be just a promotional method for the studio, and in the end, other low-cost methods will be used to complete the traffic manipulation.

2.5. Comparison of advantages and disadvantages of manipulate mode

The above five traffic manipulation modes each have their own advantages and disadvantages. Let us conduct a comparative analysis on them:

Advantages and disadvantages of each manipulation mode

Mode	Advantages	Disadvantages
Protocol cracking	Fast ramp-up; meets clients who need large play counts quickly.	Needs a team with strong reverse-engineering and attack-defence skills, a technical barrier; volume can be unstable and may drop later.
Device farms	Combines device-information changes, fake locations and automated scripts with device-spoofing tools and proxy IPs, partly solving the difficulty of protocol cracking and the slowness of manual work.	Requires buying a number of device-farm units; equipment costs are high.
Idle-client traffic	Traffic comes from all over the country; source IPs are real user IPs.	Efficiency depends on how many users run the idle client and how widely it is installed.
Multi-window	Opens many video windows to inflate plays; relatively low technical difficulty and cost.	Relatively slow.
Manual	Entirely real users; cannot be detected by technical means.	Order dispatch and settlement are cumbersome and depend on the studio's own members; slow and relatively costly, so only suits clients who require genuinely valid plays.

Advantages and disadvantages of the five manipulation modes

Source: Threat Hunter original report, page 21. Table re-typeset in English from the original.

2.6. Flushing characteristics and anti-fraud strategies

Based on the offensive and defensive confrontation between mainstream video platforms and traffic manipulation gangs, we have summarized the following characteristics of traffic manipulation:

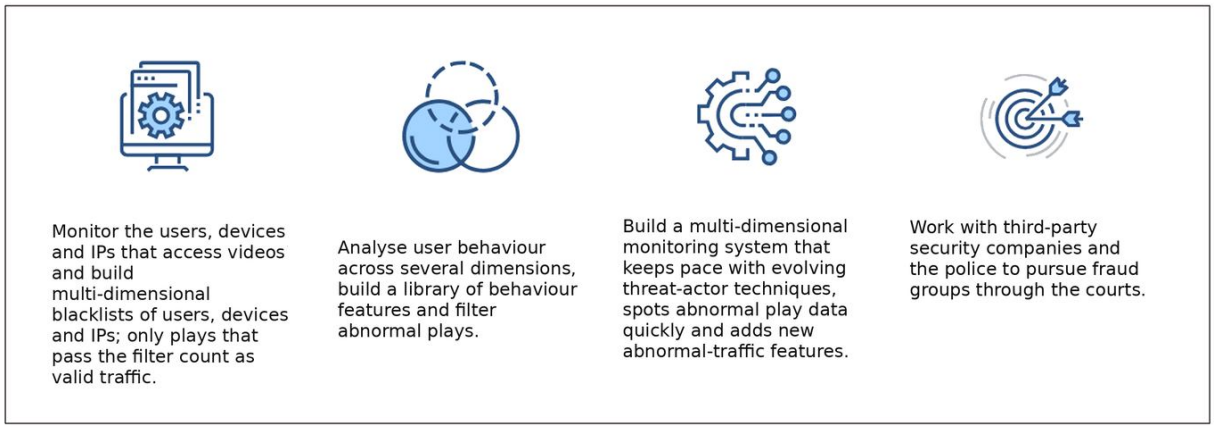
Platform detection dimensions and how manipulation groups evade them

Platform detection dimension	How manipulation groups counter it
User ID	Register many accounts with SMS code services, CAPTCHA solving and sign-up bots; buy member accounts in bulk; rent shared accounts.
IP	Keep switching IPs with proxy IPs and fast-redial devices.
Device fingerprint	Change phone fingerprints with hardware-spoofing software; forge device information with emulators.
Cache	Clear the cache or use private browsing and watch again, which counts as a new play.
Browsing behaviour	On some platforms opening the video page counts as a play, so click-simulation tools open and close the page repeatedly.
Plays of highly relevant segments	Play the segments most relevant to the video content.
Playback behaviour	Simulate the growth curve of real plays, such as the relation between plays and time.

Platform detection dimensions and how manipulation groups counter each one

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

There has always been an offensive and defensive confrontation between video platforms and cybercrime ecosystem. The following is the anti-fraud strategy suggested by Threat Hunter:



Anti-fraud measures for video platforms

Source: Threat Hunter original report, page 22. Original figure with Chinese text replaced by English.

3. Analysis of online video traffic fraud cybercriminal groups

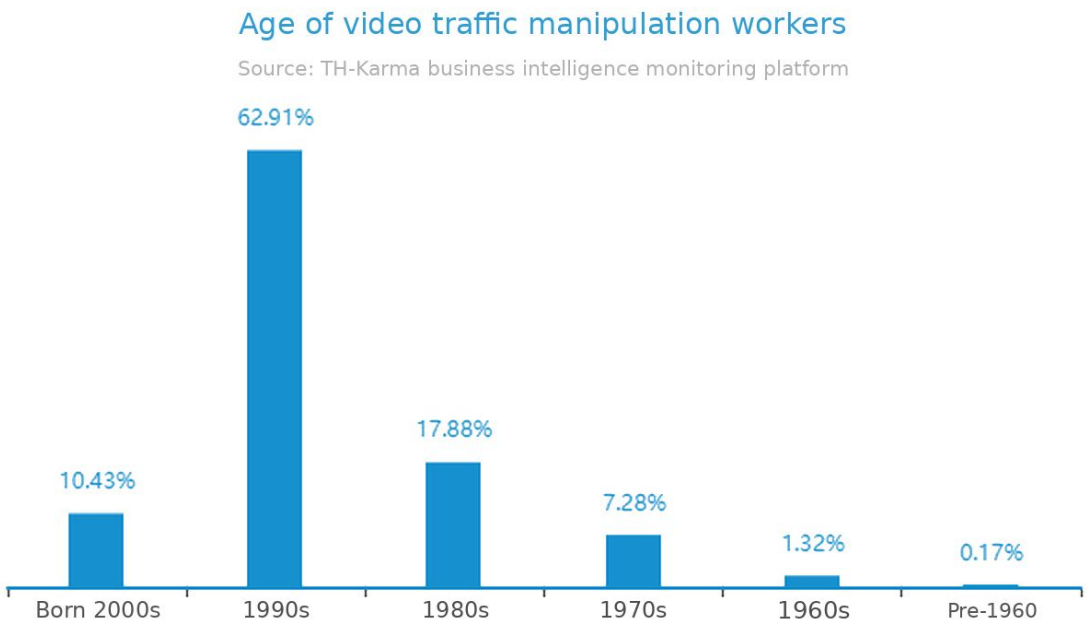
3.1. manipulate cybercrime operators group data

3.1.1. Size

Through long-term monitoring of the cybercrime ecosystem business of video traffic manipulation, Threat Hunter came into contact with video traffic manipulation-related groups, and took the initiative to contact multiple large traffic manipulation gangs and studios. It learned that a large studio spent more than one million yuan per month to maintain servers and purchase accounts, but it could be paid back quickly. It was speculated that there are currently hundreds of thousands of cybercrime operators engaged in video traffic manipulation, with an annual output value of billions of yuan.

3.1.2. Age level

Judging from the age distribution, the amount of traffic manipulation practitioners are mainly concentrated in the post-90s generation, accounting for more than 60% of the employees. The post-90s generation is not only the main force of contemporary consumption, but also the main force of the contemporary cybercrime ecosystem. As the first batch of people born in the 1980s to come into contact with the Internet, they also account for nearly 20% of the cybercrime ecosystem. Details are shown below:

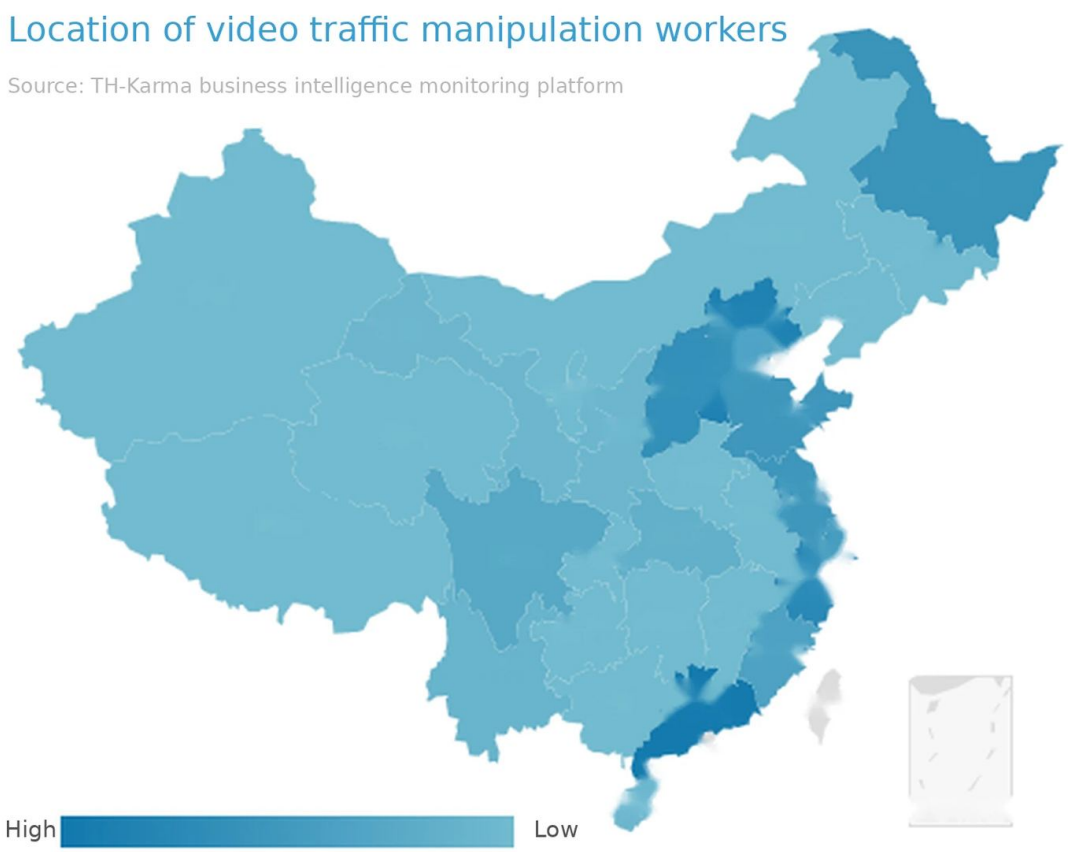


Age of video traffic manipulation workers: 62.91% were born in the 1990s

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

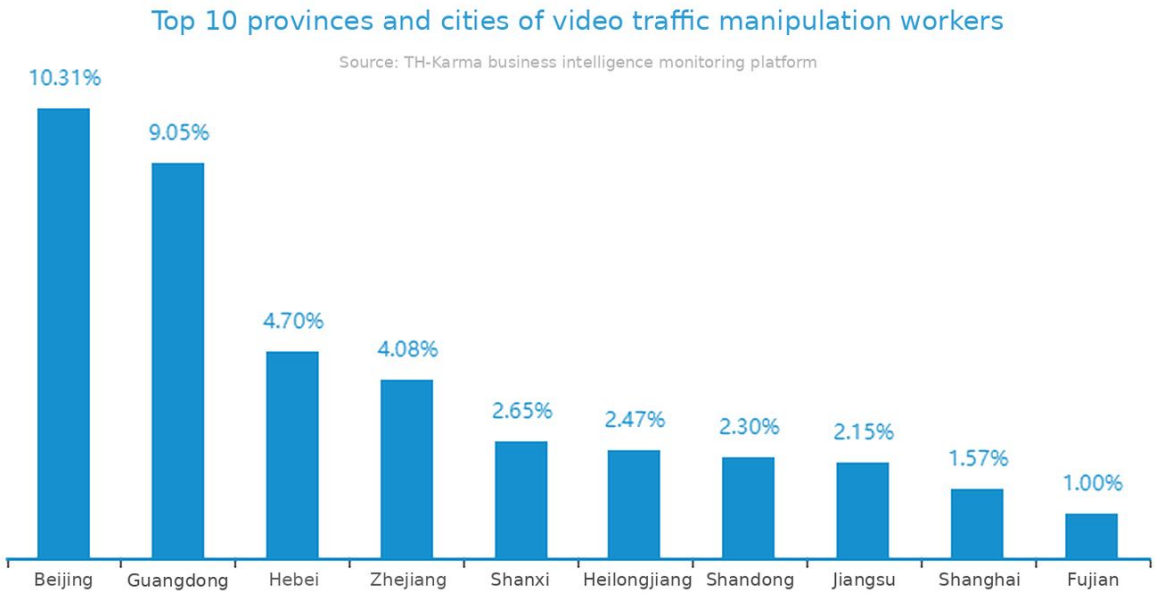
3.1.3. Geographical distribution

The figure below shows the geographical distribution of traffic manipulation practitioners. It can be found that traffic manipulation practitioners are concentrated in the eastern region of China, with Beijing, Guangdong, Hebei, Zhejiang, and Shanxi occupying the top five in the geographical distribution list, which is basically in line with the level of economic development and population density distribution. It can be seen that the more economically developed areas are, the more Internet crimes occur. Relatively speaking, in economically underdeveloped areas, the use of Internet crimes has not yet formed a large scale. Details are shown below:



Where video traffic manipulation workers are located: darker regions have more workers (see the chart of the ten leading provinces below)

Source: Threat Hunter original report, page 24. Original figure with Chinese text replaced by English.



Top 10 provinces and cities of video traffic manipulation workers

Source: Threat Hunter original report, page 25. Original figure with Chinese text replaced by English.

3.2. Mostly studio format

Most of the practitioners working in traffic manipulation exist in the form of studios. Studio members have a clear division of labor and have their own technical teams, operations teams, sales teams, etc. The number of studio members ranges from dozens or even hundreds depending on the company's business scope.

Let’s take a certain studio as an example, which shows its team member structure in detail:

Team structure of one manipulation studio (number of people)

Business team	Project director	Pre-sales	Planning	Copywriting	Execution and reporting
Zhihu (12)	1	3	3	3	2
Douban (9)	1	3	1	2	2
Xiaohongshu (11)	1	3	2	2	3
WeChat (13)	1	3	3	3	3
Weibo (10)	1	3	2	2	2
Other (19)	1	5	5	4	4

Team structure of one manipulation studio by platform team

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

3.3. Diversification of business types

Studio groups engaged in online video sales often do not just engage in a single business, but involve many business areas, such as microblogs, news websites, official accounts, apps, lifestyle-sharing communities, short-video apps and other promotion businesses, and can even undertake foreign market promotions. The business scope is obviously profitable. Today's hot short video and live broadcast industries, beauty apps, etc. are the business lines that cybercrime ecosystem studio focuses on promoting. The following are examples of business that a studio group can undertake:



Business keywords of manipulation studios: website traffic, short video, official accounts and more

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

Examples of businesses that a P2P traffic on-hook platform can undertake:

Services offered by a P2P idle-client traffic platform

Service	Description
News sites, advertorials	Covers tens of thousands of media outlets across all industries nationwide.
App home-page smart recommendation	Smart recommendation for CNY 600, 100,000+ reads, back-end data provided.
WeChat official accounts	Covers official accounts in every industry across the internet.
KPI data maintenance	Video sites, Weibo, WeChat, bullet comments, shares, comments, likes and more.
Xiaohongshu	Beauty and parenting KOLs, ordinary users and influencers; original notes and videos; trending placement.
Video site home-page promotion	Home-page promotion on major video sites (iQiyi, Sohu Video, LeTV, Tencent Video, bilibili, AcFun, etc.).
Douyin	Influencer accounts; prices updated in real time.
Zhihu	KOLs, data maintenance, Q&A, likes and comments.
Weibo trending topics and hot searches	The topic lists and hot searches with the most traffic, run by a professional team.
Douban	Rating up and down, KOLs.

Services offered by a P2P idle-client traffic platform go far beyond video plays

Source: Threat Hunter original report, page 26. Table re-typeset in English from the original.

3.4. Rapid technological updates

Professional volume traffic manipulation practitioners can be said to be well aware of the fraud controls details of video websites, such as how many times a certain video platform will adjust parameters in a week, how often data will be reset, etc. In addition to the platform security team itself, volume traffic manipulation gangs may be the group that pays the most attention to platform fraud-control strategies. cybercrime ecosystem fraudsters usually work as a team and have independently developed technologies and platforms. They can respond to the platform's updated fraud-control strategies in a timely manner and develop new fraud algorithms.

Take a registration machine tool for a certain video platform. This tool has been updated iteratively, and the update frequency can reach up to 5 versions a day. Each update means a confrontation between the cybercrime ecosystem and the platform:

Versions of a sign-up tool for one video platform

MD5	File name	First seen
e686aa1f978c386f56a9d30a4d2f839c	[author tag] Invite sign-up v1.81-[blurred].exe	2018/12/3 21:30
6df28de6db7a03192403ad15e3da9269	[author tag] Invite sign-up v1.8-[blurred].exe	2018/12/3 0:32
7b6780a0c22233b0e8f8855fd45ab209	[author tag] Invite sign-up v1.781-[blurred].exe	2018/12/3 0:01
73e18f35f09df1632e07bdf1a23b0ee2	[author tag] Invite sign-up v1.771-[blurred].exe	2018/12/2 21:33
c63e758af22a0d5aabaf15f9d21716f8	[author tag] Invite sign-up v1.77-[blurred].exe	2018/12/2 20:30
0d04bdeca5249f8b29e85a2086cde323	[author tag] Invite sign-up v1.76-[blurred].exe	2018/12/2 20:05
717f5fe9231a315215aba7e5ab8eb711	[author tag] Invite sign-up v1.75-[blurred].exe	2018/12/2 19:14
57474a1794abc84098cb054ec466d2f7	[author tag] Invite sign-up v1.75-[blurred].exe	2018/12/2 19:09
78a8e1459d4c45c3bb16e9bc466d9e5b	[author tag] Invite sign-up v1.75-[blurred].exe	2018/12/2 19:04
f49dd7b8908c4b69c4fdb2b65aa91b11	[author tag] Invite sign-up v1.73-[blurred].exe	2018/12/2 17:11
90704e71f31daa66e773d619575a6255	[author tag] Invite sign-up v1.73-[blurred].exe	2018/12/2 17:09

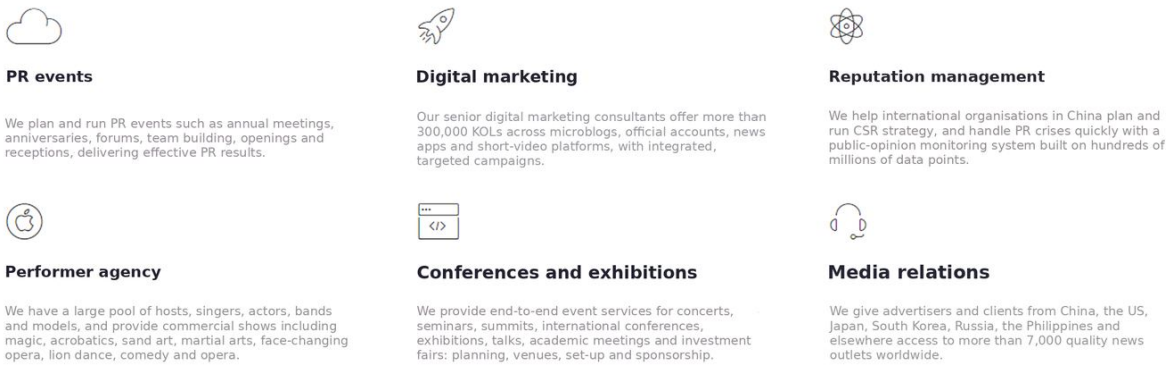
A sign-up tool for one video platform was updated many times within two days

Source: Threat Hunter original report, page 27. Table re-typeset in English from the original.

3.5. Wandering in the gray area

Unlike telecommunications fraud, illegal trafficking of citizen information, etc., which are clearly illegal and criminal in nature, fraud has always wandered in the gray edge of the law. Some studios that are engaged in normal business such as advertising promotion, marketing, public relations activities, etc. will also undertake traffic manipulation business, and the traffic manipulation business is packaged as the so-called video data maintenance business, and the studio has formal registration information and website, and some studios can also provide contracts and formal invoices. For example, the picture below shows the business scope and introduction displayed on the official website of a video traffic manipulation studio:

Among them, the digital marketing business involves gray businesses such as video traffic manipulation:



A marketing firm presents its services, with video traffic manipulation folded into digital marketing

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

Digital marketing projects offered by one firm

Digital marketing project	Description
Video traffic	Traffic data maintenance for video sites: safe, stable and efficient.
Zhihu promotion	Institutional account operation, topic ranking pushes, trending amplification.
Douban promotion	Professional film and TV reviews, promotion, discussion-board maintenance.
Xiaohongshu promotion	Let conversion rates and service speak; a must for marketplace merchants.

The firm's digital marketing projects include video traffic

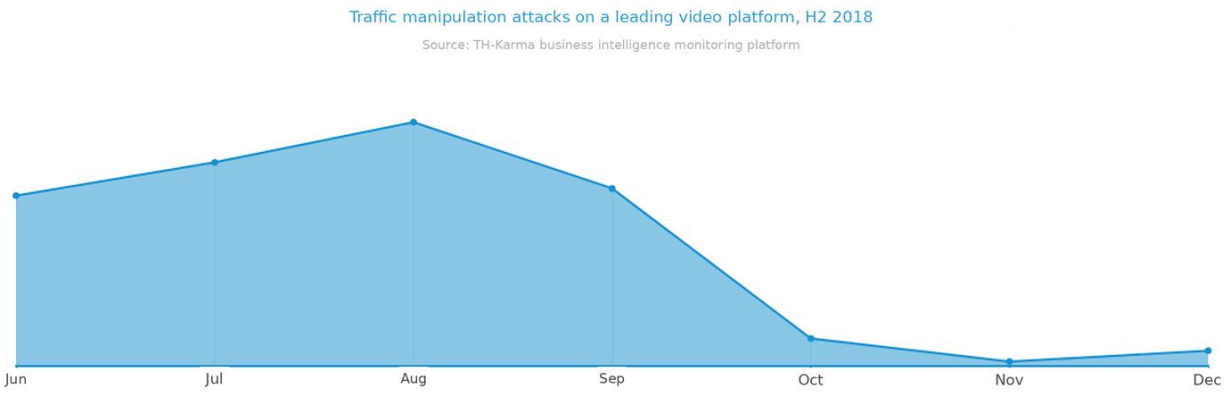
Source: Threat Hunter original report, page 28. Table re-typeset in English from the original.

4. Write at the end

In the traffic war, whose cheese is moved by the video volume?

The report pointed out at the beginning that no matter whether it is video platforms, advertisers, or producers, they are all victims in the long run. In the entire video traffic game, cybercrime operators may be the only beneficiaries. However, at the current stage, due to various reasons, some groups want to fight against the cybercrime ecosystem, but are limited by resources and capabilities and are "powerless"; on the other hand, some groups destroy the market competition environment for short-term self-interest, turn a blind eye to the cybercrime ecosystem behavior, and even contribute to the flames behind the scenarios, fueling the arrogance of the cybercrime ecosystem.

Fortunately, there are already online video platforms that have taken the lead and continue to actively fight against the cybercrime ecosystem, and the results are remarkable. The picture below shows the trend of video traffic manipulation attacks suffered by a leading video platform in the second half of 2018. As the platform launched a new strategy in September 2018, including closing the display of front-end playback volume, traffic manipulation attacks once fell off a cliff:



Traffic manipulation attacks on a leading video platform fell in the second half of 2018 after it adjusted play counts and countermeasures

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

However, the active confrontation of a few platforms cannot deal a serious blow to the amount of cybercrime ecosystem videos. The entire industry needs to join forces to jointly purify the market environment.

From the perspective of the entire Internet content industry, volume traffic manipulation is a black sheep that must be eliminated. The healthy and sustainable development of the Internet content industry depends on the long-term mutual attention and trust between stakeholders such as content display platforms, content providers, advertisers, and users. As a professional third-party cybercrime ecosystem intelligence research institution, Threat Hunter will continue to pay attention to the development and changes of the traffic manipulation industry chain, and work with all parties to create a healthy and clean market environment for the Internet content industry.

Description

1. About business intelligence monitoring platform TH-Karma:

Business intelligence monitoring platform TH-Karma is a business intelligence monitoring platform based on Threat Hunter's real-time control of cybercrime ecosystem. It adopts multi-dimensional data collection and in-depth intelligence processing systems to provide enterprises with the most timely and effective panoramic business risk perception capabilities, helping enterprises to detect business risks at an early stage and quantify their impact on the business. It can continue to conduct multi-dimensional monitoring of threat actors and serve as business risk scouts for enterprises.

2. About Threat Hunter:

Threat Hunter is an innovative security company that specializes in business security intelligence capabilities. It aims to provide customers with business attack and defense intelligence and a full range of business security solutions from prevention and control to attack. Since its establishment, the company has invested a lot of resources to build a set of domestic leading business security intelligence monitoring and early warning systems, forming a strong cybercrime ecosystem surveillance and control capability, and providing customers with cybercrime ecosystem intelligence and business fraud controls solutions. Currently, it has provided services to nearly a hundred of the country’s top Internet companies.

3. Contact information:

Business cooperation: th-business@threathunter.cn Reprint authorization: th-marketing@threathunter.cn Official website of the company: www.threathunter.cn Contact number: 0755-2660 0293 Company address: Room K, 15th floor, Building 3, Xunmei Technology Plaza, Kehua Road, Nanshan District, Shenzhen, Guangdong Province Welcome to follow the Threat Hunter official account to obtain more professional reports