

黑产大数据

在线视频流量欺诈黑灰产研究报告

威胁猎人鬼谷实验室

报告声明

本报告由威胁猎人鬼谷实验室独家编写与发布，报告中所涉及的数据取自威胁猎人 TH-Karma 业务情报监测平台和互联网公开数据。受限于数据来源、取样方式以及分析方法等因素，本报告中的相关内容与实际情况之间可能存在一定的误差。

本报告版权属威胁猎人（深圳永安在线科技有限公司）所有，并受法律保护，未经许可不得擅自转载、修改或利用其他方式使用报告文字或者观点，如需转载请联系威胁猎人授权。

目 录

1.	报告概述	1
1.1.	内容简介	1
1.2.	报告要点	2
2.	在线视频流量欺诈黑灰产行业现状	3
2.1.	刷量黑灰产业现状概述	3
2.2.	刷量黑灰产业存在原因	6
2.2.1.	市场急功近利，需求远大于供给	6
2.2.2.	高回报与低风险	6
2.3.	刷量黑灰产业链概述	7
2.3.1.	会员模式与访客模式	7
2.3.2.	刷量价格	10
2.4.	刷量方式详解	10
2.4.1.	协议破解：上量高效迅速	10
2.4.2.	群控：群控升级，黑灰产运营成本降低	12
2.4.3.	流量挂机：流量来自全国各地真实用户 IP	14
2.4.4.	多开模式：技术门槛最低	16
2.4.5.	人工刷量：流量真实有效，难以检测	17
2.5.	刷量模式优缺点对比	18
2.6.	刷量特征与反欺诈策略	19
3.	在线视频流量欺诈黑灰产团伙分析	20
3.1.	刷量黑灰产人员群体数据	20
3.1.1.	规模大小	20
3.1.2.	年龄层次	20
3.1.3.	地域分布	21
3.2.	多为工作室形式	22
3.3.	业务种类多样化	23
3.4.	技术更新快	24
3.5.	游走在灰色地带	24
4.	写在最后	25

1. 报告概述

1.1. 内容简介

一部影视剧火不火，收视率和播放量似乎成为最直观的指标，太多无论热门与否的在线视频，播放量都能够轻松过亿，影视团队动辄过亿甚至百亿的宣传通稿，似乎彰显着在线影视剧播放量进入百亿时代。

在线视频影视行业蓬勃发展的背后，值得深思的是漂亮的数据背后到底孰真孰假，假数据到底又能带来怎样的恶劣影响。

对于视频平台，刷量所带来最直接的影响，是内容版权分销和付费增值服务资金的损失。其次，如今在线视频行业由传统免费模式逐渐转变为用户付费模式，通过引进优质内容，打造品牌口碑，才能抢占付费会员阵地，而虚假数据的背后，直接干扰了平台对优质内容的引进，影响用户体验导致平台付费用户流失。

对于广告主，播放量的造假会造成 IP 估值与实际背离，广告商、投资商的项目评估被掺水，不仅广告资金损失没有达到预期的转化效果，长此以往必将会导致商业模式的扭曲和市场的亚健康。

对于制片方，表面上作为其中的受益者，其实不然。即便一时获得了炫目耀眼的业绩，也不过是一种自我安慰和麻醉罢了，当制片方不知道哪一类内容是真正受用户喜欢，会对整个影视业带来恶性循环。

不可否认，在线视频虚假播放俨然成为整个行业的痛点。

本报告的重点研究对象为在线视频（长视频）刷量黑灰产业，短视频、直播等其他视频形式相关的黑灰产不在本报告的重点研究范围内。本报告基于威胁猎人的黑产大数据，期望以客观和详实的数据反映当前在线视频流量欺诈的现状，并深入挖掘隐藏在其背后的黑色产业链，从分工内容与模式、刷量成本与收益、刷量方式与方法、团伙特征等多个维度进行阐述和分析。

1.2. 报告要点

- 刷量主要活跃在头部在线视频平台，从刷量流量占比来看，前三分别为腾讯视频（34.11%）、爱奇艺（27.41%）和优酷（18.55%）。
- 从被刷量的视频类型数据来看，电视剧因剧集多，刷量总数大，因而刷量占比最大，达到 72.69%；对于电影而言，更侧重于在上映前后通过刷预告片、宣传片或片花的播放量来提高电影的曝光量，而不是直接刷电影的播放量。
- 从刷量流量源 IP 角度分析，超过 99.95% 的流量源于国内 IP，覆盖国内各个省市自治区，但有明显的地域聚集倾向，归属于江苏省和北京市的 IP 数量超过了 50%。约有 1/4 的视频刷量流量源 IP 归属于各地的 IDC 机房，且绝大部分为腾讯云主机和百度云主机。
- 研究推测，目前从事在线视频刷量的黑灰产从业人员数十万人，年产值数十亿元。刷量从业人员主要集中在 90 后，比例超过 60%，且集中于我国东部地区。刷量人员多以工作室形式存在，业务种类多，技术更新快，且视频刷量方式多样，特征不一，各有优缺点。数据造假热度由早期的电视收视率造假，转为在线视频播放量造假，而目前在线视频刷量的热度也正在向短视频、直播行业转移。
- 已经有在线视频平台率先并持续性地与视频刷量黑灰产进行着积极地对抗，并且效果显著，但是少数平台的积极对抗并不能给整个视频刷量黑灰产予以重创，需要整个行业通力合作，协同打击。

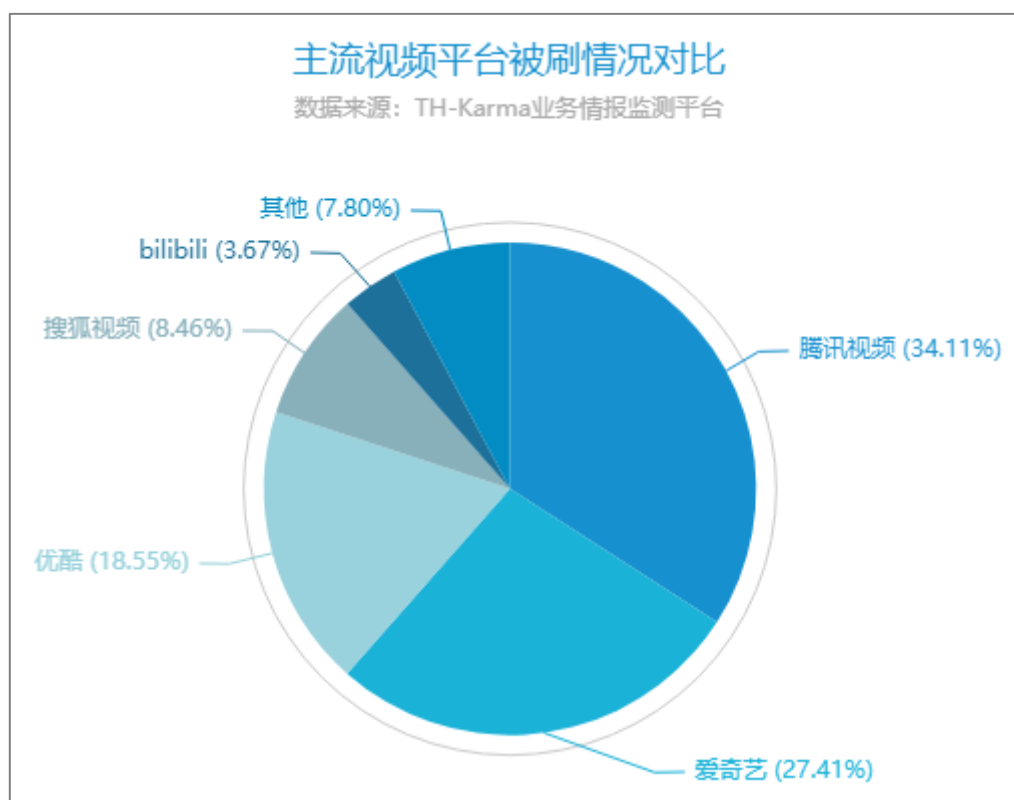
2. 在线视频流量欺诈黑灰产行业现状

2.1. 刷量黑灰产业现状概述

艾瑞咨询预测，我国在线视频行业市场规模预计 2020 年达到 2129.7 亿元，预计 2016 年到 2020 年的年复合增长率为 34.98%。巨大的行业市场产值，除了吸引了众多视频内容创作者投身其中，也引起了刷量黑灰产人员的注意。加之法律、监管制度尚待完善，刷量的犯罪成本低、短时间内回报高，吸引大量人员投入到视频刷量的黑灰产业当中。研究推测，目前从事视频刷量的黑灰产从业人员数十万，年产值数十亿元。

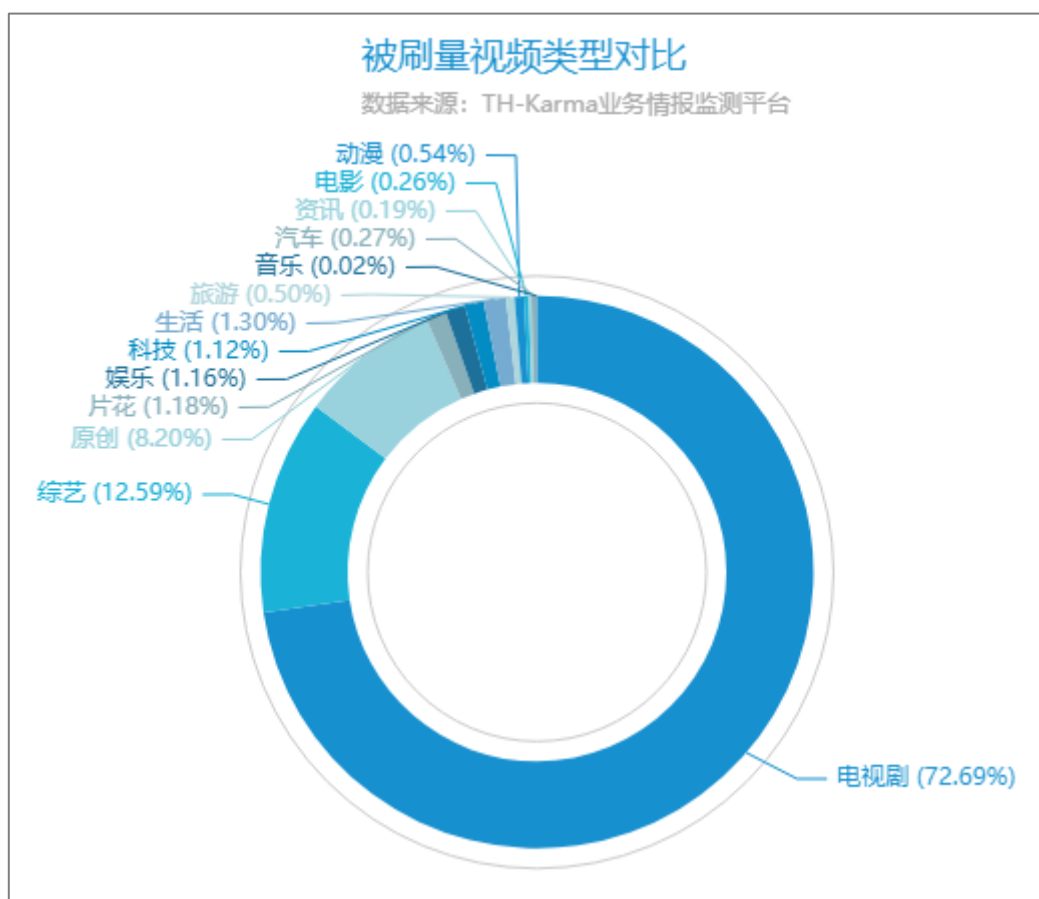
虽然少数视频平台针对虚假播放量做出积极对抗，如爱奇艺加强了反刷措施，并宣布关闭前台播放量展示，向“唯播放量”论发起挑战，在一定程度上减少了播放量欺诈行为，但是并没有对整个视频刷量黑灰产业造成太大的影响。

通过威胁猎人 TH-Karma 业务情报监测平台长期捕获的视频刷量数据来看，被刷量平台主要集中在腾讯视频、爱奇艺、优酷、搜狐视频、bilibili 等已占据较大市场份额的头部平台，如下图所示：

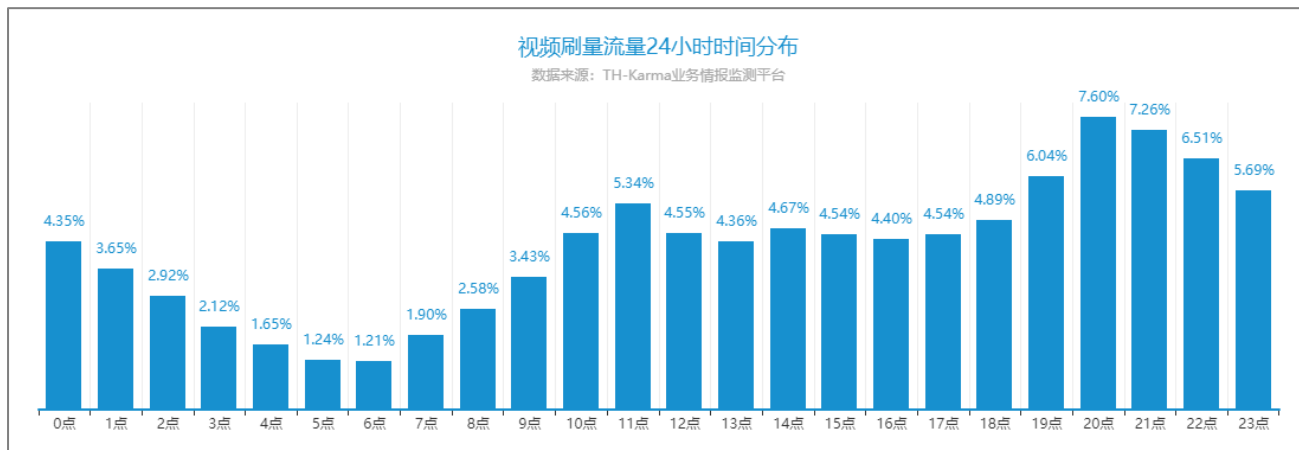


究其原因，这些头部平台视频分成机制更加完善，刷量不仅可以牟取更多的视频分成，也可以达到更好的推广效果。

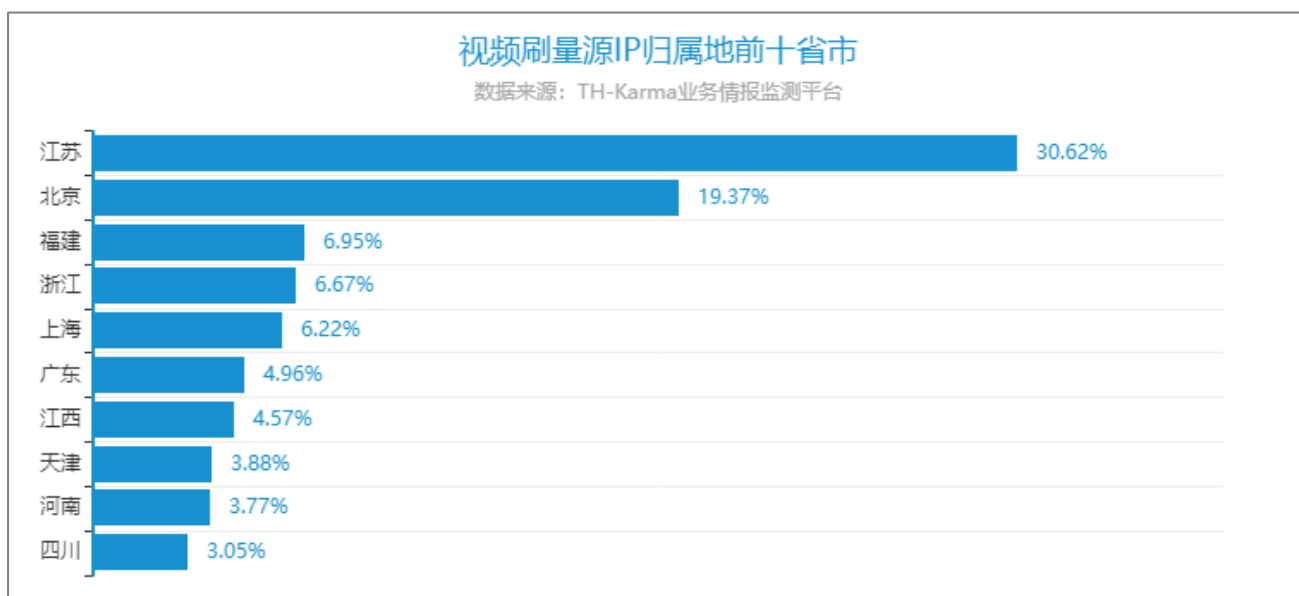
从被刷量的视频类型数据来看，电视剧因剧集多，刷量总数大，因而刷量占比最大，达到 72.69%；对于电影而言，更侧重于在上映前后通过刷预告片、宣传片或片花的播放量来提高电影的曝光量，而不是直接刷电影的播放量，详情见下图：



黑灰产的攻击行为会模仿真实用户的行为，以增加厂商对异常流量识别的难度。不论是视频刷量黑灰产，还是广告点击欺诈、文章阅读量造假等，刷量流量会尽可能地符合大众真实用户的访问习惯。下图展示了视频刷量流量 24 小时内的时间分布情况，刷量高峰时间段为夜间 19 至 23 点，并在黄金时间 20 点达到最高值：



从视频刷量流量源 IP 角度分析，超过 99.95% 的流量源于国内 IP，广度覆盖国内各个省市自治区，但有明显的地域聚集情况，视频刷量的源 IP 中，归属于江苏省和北京市的 IP 数量超过了 50%。约有 1/4 的视频刷量源 IP 归属于各地的 IDC 机房，并且绝大部分为腾讯云主机和百度云主机。视频刷量源 IP 归属地前十省市统计如下图所示：



另外，威胁猎人近期监测到，于 2018 年 12 月 27 日在某视频平台开播的由多个当红流量小生参演的电视剧《*风刀》，开播起一个月内在存在上亿次虚假刷量；泰国电影《降服**的手段》于 2019 年 1 月 16 日上映，某泰语翻译字幕组作为幕后推手，欲通过制造每日上千万的宣传片虚假播放量，提高该电影的曝光度。

2.2. 刷量黑灰产业存在原因

2.2.1. 市场急功近利，需求远大于供给

在线视频虚假播放量背后牵扯着多方利益，远大于供给的刷量需求，是视频播放量欺诈行为屡禁不止的主要原因。在线视频行业主要涉及三大角色，视频平台、广告投资商、制片方。

制片方是对视频播放量需求最大的一方。最直观的目的，是可以获得视频网站更多的流量和视频分成。高播放量可以提升排名，吸引更多用户观看，自然可以获得更多的流量。对于视频分成，主要包括广告期分成、内容分成、会员付费期分成，而有效的播放量是结算的重要指标。

其次，某些片方与广告主签订了对赌协议，刷量不仅可以避免承担对赌失败的风险，同时虚高的数据也是后续招商的重要资本。

在 IP 为王的如今，刷量不仅可以辅助片方打造出一部“爆款”影视剧，或者力捧导演与明星，随之高热度 IP 流量也可带来巨大的附加价值与资源。

刷量可以说是最简单也最立见功效的贴金手段。对于没有大牌明星，没有过硬班底，很多时候网络影视的制作方甚至没有宣传的人力物力，相比其他昂贵的营销推广方案，几元至几十元包一万的访问量可以说是简单高效，但换来的点击分成或贴片广告的价值，却远远溢价。在这种急功近利的模式之下，也就不难理解，为何刷量现象屡禁不止。

2.2.2. 高回报与低风险

在我们调查研究的过程中，接触到了某 P2P 挂机刷量平台用户 A。用户 A 向我们介绍了他如何通过挂机刷量的方式日入千元。用户 A 告诉我们，他在大量机器上部署了超过 3000 个挂机客户端，平均每日挂机收益百万以上积分。虽然该平台不支持挂机积分直接提现，但是他可通过转赠给其他用户积分的方式间接变现。按照平台充值 10 元钱=10000 积分的规则估算，用户 A 确实可以轻松日入千元。下图为用户 A 向我们展示的近期挂机积分收益（关于挂机刷量的详细内容，详见第 2.4.3 节）：

会员：

@qq.com

积分：48228

vip1

充值

充值未到账

挂机赚分

收费标准

账户设置

我要提现

挂机：3064

今日挂机赚分

85089分

在线时长4754小时

已发

最近7天任务消耗、挂机赚分统计

日期	2019-01-25	2019-01-24	2019-01-23	2019-01-22	2019-01-21	2019-01-20	2019-01-19
任务消耗统计	0	0	0	0	0	0	0
挂机赚分	85089	11356	11180	11285	112016	113524	105692

用户 A 只是庞大的刷量大军中的一个小小的缩影，对于刷量从业者来讲，敢于铤而走险大肆刷量，一方面是可以快速获取巨额利润，另一方面则是违法成本低。这条产业链上的每个环节基本都是暴利，上游卡商月入超十万甚至百万，刷量工作室都号称每天至少可刷千万级播放量，非法获利也十分可观。但是目前针对视频刷量的法律并不完善，国内首例针对刷量的起诉案件中，某刷量公司对爱奇艺网站至少造成了 9.5 亿次虚假访问，该公司也承接其他主流视频平台的刷量业务，保守估计非法获利百万以上，但最后仅判赔 50 万。

2.3. 刷量黑灰产业链概述

2.3.1. 会员模式与访客模式

目前主流的视频播放分为两种模式，一是会员登录播放，二是访客模式。两种播放模式下也滋生了两条不同但都分工明确的刷量产业链。

对于会员模式刷量产业链，整个产业链条可以分为下图所示的上中下游三大模块：



会员模式要完成视频刷量，首先要注册大量的平台账号，对上游账号注册环节具体分析如下：

(1) 角色与资源

- a) 卡商：多以正常业务为幌子，通过各种渠道从运营商或代理商处获取手机卡资源，然后加价出售给下游卡商、接码平台、下游号商赚取差价。其提供的手机卡按类型可分为：虚拟卡/实卡、语音卡/短信卡、海外卡/国内卡、流量卡/注册卡。
- b) 接码平台：负责连接卡商和有手机验证码需求的群体，提供软件支持、业务结算等平台服务，通过业务分成获利。
- c) 打码平台：主要用来识别图片验证码的平台。在注册视频网站账号的时候，一般会用各种形式验证码来防止机器批量注册，打码平台可以破解这个限制。打码平台可以用软件机器打码，也可以招聘“码工”人工打码。
- d) 代理 IP：代理 IP 平台提供大量代理 IP 资源，使用代理 IP 作为跳板，可以隐藏自己真实的 IP。通过不断切换 IP，可以绕过视频平台在 IP 维度的风控策略。

e) 秒拨机：秒拨机可以理解为拨号 VPS，即动态拨号虚拟机，可以通过宽带拨号来切换 IP。相对于代理 IP，秒拨机拨出的 IP 为真实宽带拨号 IP，对于视频平台来说更难检测和防控。

(2) 成本及利润分析

a) 卡商：根据手机卡类型不同，每张手机卡价格不同，部分卡类型平均价格如下：

卡类型	虚拟运营商号段		传统运营商号段		真人实名卡
	批发	零售	仅短信功能	含语音功能	
价格(元/张)	5	10	14	20	100

卡商将黑卡接入接码平台，提供接受手机验证码的服务，根据注册项目不同，每个手机验证码可以获得 0.01 元至 3 元不等的收入。

- b) 接码平台：除了平台本身的手机卡接码获利以外，另一部分收入为接入卡商收发验证码的收入分成，一般为 30%左右。
- c) 打码平台：打码价格根据验证码类型及其复杂程度有所不同，以下为某打码平台价格示例：

验证码类型	4位纯数字	4位纯英文	4位数字英文	4位汉字	计算题
价格(元/个)	0.01	0.01	0.01	0.04	0.014

刷量工作室会从软件开发商购买批量注册爱奇艺、优酷、腾讯视频等视频平台的注册机工具，结合接码平台与打码平台，快速批量注册平台账号，部分工作室也会直接向号商购买大量平台会员账号。最后通过协议破解类刷量工具、群控或者人工刷量等方式，对视频进行播放、点赞、评论等操作。

对于访客模式刷量产业链，与会员模式产业链最大的区别就是，完成视频刷量无需登录账号。访客模式下，对于黑灰产团伙来说，减少了的刷量过程中的账号成本，但对于视频平

台来说，缺少用户 ID 这一检测维度，提升了刷量行为的检测难度。通过对刷量团伙的调研分析，访客模式为目前的主流刷量模式，具体刷量手段详见第 2.4 节。

2.3.2. 刷量价格

刷量价格与平台大小和平台风控规则相关，我们综合不同刷量团伙的报价，统计出各大视频平台的刷量平均价格，如下所示：

网站名称	播放量(元/万次)	订阅粉丝(元/万个)	赞/踩(元/万次)	评论(元/条)	弹幕(元/条)
YOUKU	4	110	70	0.4	0.9
爱奇艺	50	280	70	0.4	0.9
腾讯视频	4	800	/	1.4	0.7
bilibili	230	1600	/	1.4	0.9
搜狐视频	50	400	120	0.4	0.7
Acfun	2	/	200	/	/
PP视频	11	/	/	/	/
乐视视频	3	/	130	/	/
芒果TV	2	/	/	/	/
华数	2	/	/	/	/

刷量业务与刷量价格都会随着平台的风控对抗强度和有效性的变化而调整，具有较强的时效性。例如在 2018 年 7 月间，爱奇艺加强了反刷措施，部分刷量团伙一度暂停相关业务，直至有卖家宣称有独家不掉量技术，但刷量价格大幅上涨至 100 元/万次。而在 2018 年 9 月 3 日，爱奇艺宣布关闭前台播放量展示后，许多工作室表示不再承接相关业务。

2.4. 刷量方式详解

2.4.1. 协议破解：上量高效迅速

协议破解，即黑灰产通过破解客户端与服务器通信中的通讯协议与算法，伪造相应的请求及参数直接访问通信接口达到刷量目的。

以 2018 年 4 月我们捕获到的一款名为“天龙刷视频软件”的最新版工具为例，支持包括

优酷、腾讯视频、爱奇艺、芒果 TV、乐视视频等多个视频平台的刷量，如下图，软件内部针对芒果 TV 构造的 URL 和 HTTP 请求头：

.rdata:0051AD00	db	'User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:27.0) Gecko/20'
.rdata:0051AD00	db	'100101 Firefox/27.0',00h,0Ah
.rdata:0051AD00	db	'Connection: Keep-Alive',00h,0Ah
.rdata:0051AD00	db	'Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3',00h,0Ah
.rdata:0051AD00	db	'Accept-Encoding: deflate',0
.rdata:0051ADEB	aVid_0	db 'vid号',0 ; DATA XREF: sub_411F3A+7C↑0
.rdata:0051ADEB		; sub_419498+189↑0
.rdata:0051ADF1	aInvoker1Callba	db '&invoker=1&callback=playerBack',0
.rdata:0051ADF1		; DATA XREF: sub_411F3A+13E↑0
.rdata:0051AE10	aCid	db '&cid=',0 ; DATA XREF: sub_411F3A+146↑0
.rdata:0051AE16	aHttpVc_mgtv_co	db 'http://vc.mgtv.com/v2/watch?&pid=&vid=',0
.rdata:0051AE16		; DATA XREF: sub_411F3A+14E↑0
.rdata:0051AE3D	aHostVc_mgtv_co	db 'Host: vc.mgtv.com',00h,0Ah ; DATA XREF: sub_411F3A+20A↑0
.rdata:0051AE3D		db 'Accept: */*',00h,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',00h,0Ah
.rdata:0051AE3D		db 'Connection: Keep-Alive',00h,0Ah
.rdata:0051AE3D		db 'Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3',00h,0Ah
.rdata:0051AE3D		db 'Accept-Encoding: deflate',0
.rdata:0051AF1A	aCode0	db 'code':0',0 ; DATA XREF: sub_411F3A+359↑0
.rdata:0051AF22	aVideoid2	db 'videoid2',0 ; DATA XREF: sub_41232C+99↑0
.rdata:0051AF2B	aid1	db '视频id1',0 ; DATA XREF: sub_41232C+118↑0
.rdata:0051AF33	a1512108	db '1512108',0 ; DATA XREF: sub_41232C+1D9↑0
.rdata:0051AF3B	a369c147be259c0	db '369C147BE259C037',0 ; DATA XREF: sub_41232C+1E1↑0
.rdata:0051AF4C	a58	db '58',0 ; DATA XREF: sub_41232C+1E9↑0
.rdata:0051AF4F	a152pFqejiRupvi	db '152PFqeji&rupvid=&ycid=&rcid=&r_',0
.rdata:0051AF4F		; DATA XREF: sub_41232C+2B7↑0

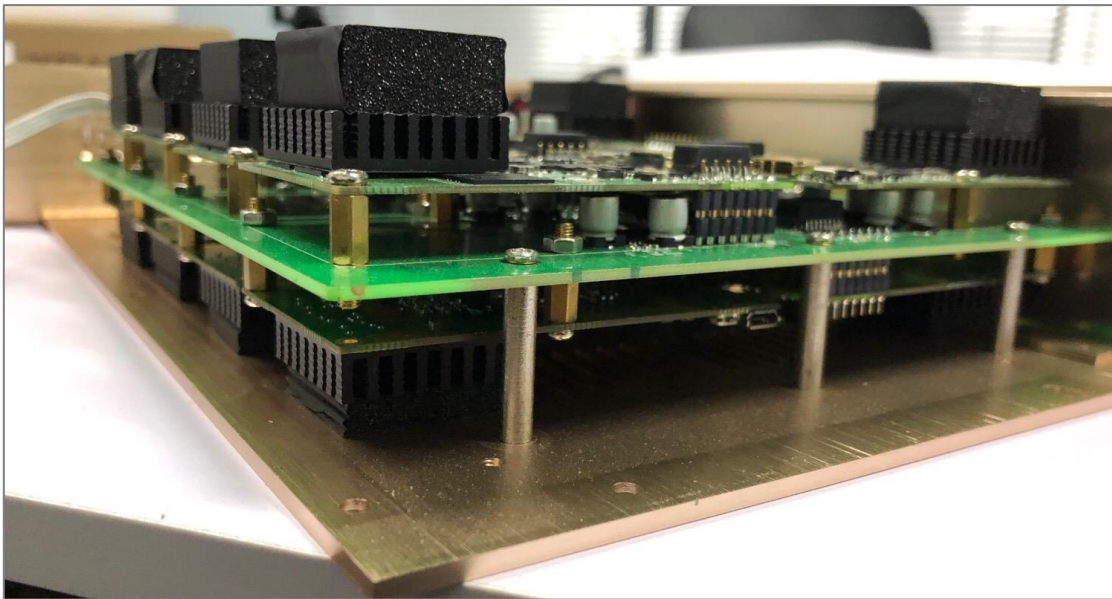
为了避免单个 IP 多次访问，这类工具还内置了拨号功能和代理 IP 网站接口。如下图，该工具可以通过内置的讯代理接口批量获取代理 IP，因此单从 IP 维度无法识别这种刷量行为：

```
.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 U0)
    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
}
```

这类工具主要通过用户购买卡密进行充值的方式进行获利，不过由于工具能被外部获取，可以通过逆向调试的方式分析出其核心逻辑，同时也有人对其进行破解放出了免费版，导致目前这类工具基本不再对外售卖，像“天龙刷视频软件”这款工具，目前已经被刷量工作室收购作为内部工具来使用。

2.4.2. 群控：群控升级，黑灰产运营成本降低

现在不少黑灰产工作室正在使用一种新型群控，我们称之为箱式群控。箱式群控是传统群控的升级变种，相较于传统群控，箱式群控不再需要外接的手机设备，而是直接将多个手机芯片封装在一个机箱中，通过网络将手机屏幕显示在控制电脑上安装的客户端内，削减了手机电池、屏幕等硬件成本，节约了占地空间，箱式群控大小仅为普通台式电脑机箱的四分之一。下图为箱式群控的内部结构：



箱式群控软硬件成套销售，箱式群控软件在稳定性、软硬件兼容性、功能完善性等方面都要明显优于传统群控软件。通过虚拟分割手机芯片内存可实现多开，每个手机芯片可裂变成为多部“手机”，可以为每个“多开手机”伪造不同的设备信息，如IMEI、手机定位、本机号码、网络信息等。也可通过电脑客户端操作批量安装App、设置代理IP、修改手机设备信息。箱式群控和传统群控优缺点对比如下：

对比项目	箱式群控	传统群控
▪ 软硬件兼容性	强	弱
▪ 配置操作复杂度	低	高
▪ 外接手机设备	不需要	需要
▪ 手机虚拟裂变	支持	不支持
▪ 硬件成本/损耗	小	大
▪ 占地空间	小	大

总之，箱式群控大大降低了黑灰产工作室的人工运营成本，同时解决了传统群控配置复杂、操作繁琐、手机电池损耗等问题。

利用群控刷量，在一定程度上解决了协议破解难度大及人工刷量速度慢的问题，利用自动化脚本批量注册和刷量的大致操作流程如下：

(1) 多台手机同时注册账号：

- 利用改机软件伪造设备指纹后打开 App 点击注册；
- 调用接码平台 API，收到并输入手机号，点击收取验证码，等待接码平台返回验证码后输入，完成注册；
- 将账号、密码及改机工具的设备信息记录到文本文件中，返回第一步进行下一轮注册。

(2) 多台手机同时刷量：

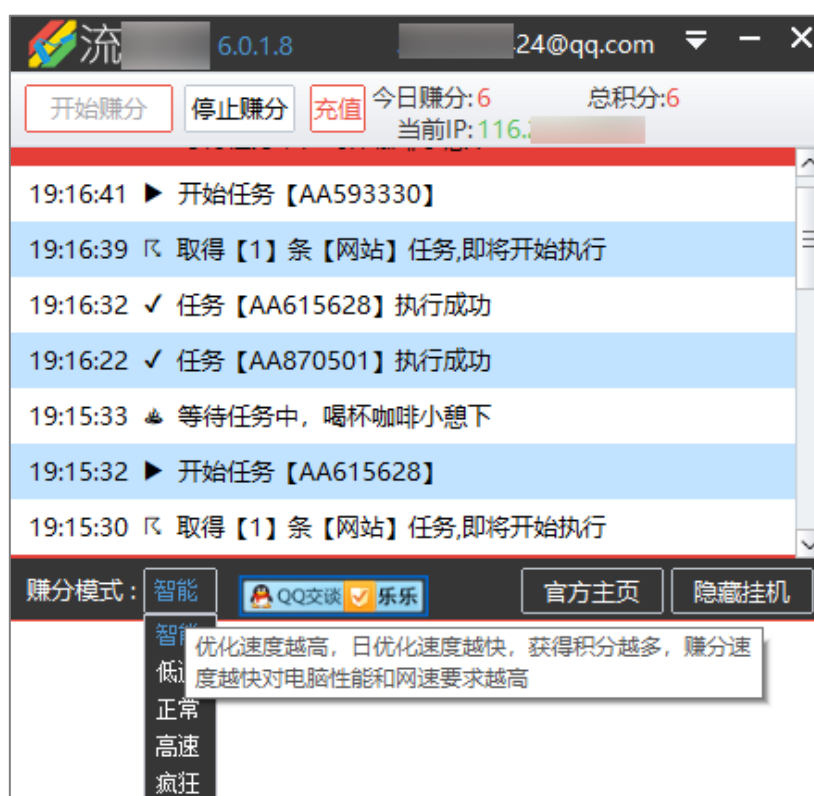
- 伪造设备指纹，打开视频 App (如有需要, 还需登录账号)；
- 搜索需要刷量的视频，打开视频，按播放设置开始刷量，完成后返回第一步进行下一轮刷量。视频播放设置包括设置播放时长、设置音量、是否连续播放、选择清晰度、自动刷新与自动清除缓存等。

2.4.3. 流量挂机：流量来自全国各地真实用户 IP

流量挂机是根据 P2P 原理来实现流量优化、视频刷量、刷排名等功能的一种数据造假模式，由两部分角色互相配合完成，挂机用户与流量需求用户。

首先由大量挂机用户下载并运行挂机软件，填入账号或挂机编号，保持在线状态，根据挂机时间和完成的任务数，可以赚取平台的积分，最后变现。而流量用户则是对推广有需求的用户，可以在流量平台上发布任务，服务器将收到的任务请求分配给挂机用户，自动完成刷量任务，且流量数据来自全国各地的真实电脑用户。

- (1) 挂机用户挂机赚分：某款挂机软件界面如下，下载并登录挂机软件后，选择赚分模式并点击开始赚分，即可自动开始获取任务并自动执行任务，任务执行成功后会获得相应的积分：



- (2) 流量需求用户发布任务：以某款流量工具为例，介绍任务发布基础设置：

- 视频链接：填写需要优化播放量的视频链接地址；
- 视频名称：填写视频链接以后会自动识别，不需要手动填写；
- 计划播放量：填写视频预刷的日播放量；
- 流量时间控制：有两种方式，分别平滑模式和高速模式：

- 平滑模式：系统 0 至 23 点之间自动分配预刷量，一般建议默认，适合不是短时间内急需大量播放量的客户；
- 高速模式：最短时间内完成用户设置的预刷量，一般预计 1 至 6 小时以内完成。适合急需短时间内快速提升播放量的用户。
- 设定好各项设置后，保存任务，点击开始可立刻优化任务。

下图为视频刷量任务设置界面：

1 基础设置 新手教程 真实效果说明

任务名称: 视频任务

视频链接: 必填

视频名称:

计划播放量: 1000 基础流量费: 2.00 点/天

流量时间控制: 平滑模式 [设置](#)

流量时间设置

☒ 平滑模式 ☐ 高速流量模式

预设总访问量: 1000 已分配访问量: 1000 未分配访问量: 0 [0至7点无流量](#) [恢复默认值](#)

访问量	46	41	36	24	17	16	22	29	33	43	47	55	58	61	60	60	57	50	44	47	48	43	36	27
时间点	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23

说明:

1. 默认流量时间曲线，符合大多数中国互联网用户的实际使用情况。
2. 启用流量时间控制，可能会降低下流量，统计到的总量达不到预设的总量，流量宝不受理此类申诉及退点申请，请酌情使用。
3. 流量控制拉杆的上限不能超过红线位置。控制杆拉到最低代表这个时间段没流量。
4. 请注意，50000访问量以上的任务，流量控制功能将无效。

[调用模板](#) [保存为模板](#) [模板管理](#)

(3) 成本及价格

对于挂机用户来说，一般单个客户端挂机 24 小时可以赚到几毛至几元不等的收益。挂机赚的收益多少跟很多因素相关，包括但不限于电脑配置、网络情况、电脑系统空闲率、服务器下发的任务数、服务器下发的任务类型、软件上的优化速度设置、软件在线时间等等。

对于流量需求用户来说，视频刷量成本根据所刷视频平台而有所不同，除了播放量基础费用外，根据设置的 IP 数量、刷量模式等，会在基础流量费用的基础上加收额外费用。以下为

某流量挂机平台针对部分视频平台的收费标准：

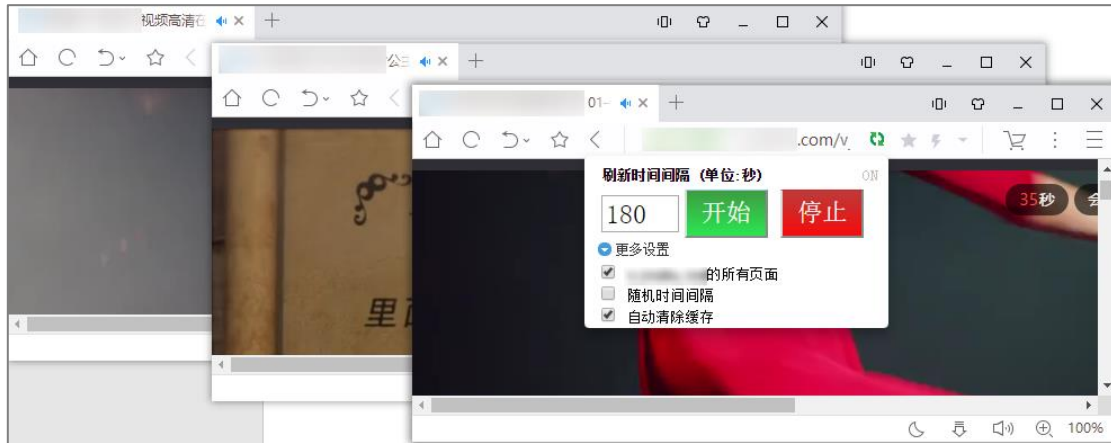
基础流量费		增值服务费
视频平台	收费标准(元/万 IP)	- IP量附加费： 超过1万IP，根据具体IP数量，加收基础流量费的20%至100% - 流量高速模式附加费： 加收基础流量费的50%
	20	
	20	
	30	
	20	
	10	
	50	
	10	
	40	

2.4.4. 多开模式：技术门槛最低

多开模式刷量主要为通过视频窗口多开，达到刷量目的。此模式相对来说，技术难度及成本较低，主要有两种方式：浏览器多开和模拟器多开。

浏览器观看视频，需要清理浏览记录及历史数据，然后开启无痕窗口，使用 Flash 播放器观看。目前以 UC 浏览器和 360 浏览器刷量较为稳定有效，具体刷量流程如下：

- (1) 打开浏览器，下载自动刷新插件；
- (2) 打开视频网站，搜索需要刷量的视频；
- (3) 设置自动刷新时间，必须大于广告时间，一般以 2 至 3 分钟为宜；
- (4) 自动刷新插件必须勾选【自动清除缓存】，设置成功后点击开始即可；
- (5) 浏览器可以根据电脑性能多开窗口同时刷量，需要将窗口拖出为独立窗口，且窗口不能最小化；
- (6) 视频播放不能静音。



通过浏览器多开刷量,对于无需登录视频平台会员账号和利用其他工具辅助即可完成的刷量,刷量可以说是零成本。按照每3分钟刷新一次,浏览器多开25个窗口来估算,每台电脑每小时可完成500次刷量。

模拟器多开是浏览器多开的优化版,通过伪造模拟器参数、结合代理IP等,可以实现在多个模拟器上同时刷量。

为解决单IP封禁问题,某代理客户端内置了老版本Chrome浏览器,可以多开浏览器,并且可以给每个浏览器分配不同的代理IP,如下图所示:



2.4.5. 人工刷量：流量真实有效，难以检测

当遇到有特定要求的视频刷量任务或刷量难度很大的时候,可以通过人工刷量的方式来完成,人工刷量分为有偿任务派单和免费平台互刷。

刷量任务派单是指,通过QQ群、贴吧等各种渠道召集真实用户,使用自己的账号对特定

视频进行观看、点赞、评论等，一个会员一个链接算一个播放量，按照链接数结算，就可以拿到每个链接 0.1 至 0.5 元不等的现金奖励。

平台互刷是在刷量互助群内分享需要刷量的视频链接，群成员按照要求互相点击，一般要求看完完整视频。

人工刷量模式完全是真实用户的真实操作，技术上是完全无法检测出来，方法简单且不存在技术壁垒，但是刷量成本相对较高，通过目前监控到的情报来看，此类模式在视频刷量上应用并不广泛。也有工作室号称其刷量方式为纯人工刷量，但是给出的报价远低于成本，这可能仅是工作室的一种宣传手段，最终还是会通过其他低成本的方式来完成刷量。

2.5. 刷量模式优缺点对比

以上五种刷量模式各有优缺点，我们对其进行对比分析：

刷量模式	优点	缺点
■ 协议破解	上量速度快，能满足对播放量需求大且快的客户。	要求技术团队具有比较强的逆向破解和攻防能力，存在一定技术壁垒，同时存在刷量不稳定的情况，后期可能会出现掉量现象。
■ 群控	群控刷量模式，集合了修改手机设备信息、虚拟定位、自动执行脚本的功能，结合改机工具、代理IP等软件，一定程度上解决了协议破解难度大及人工刷量速度慢的问题。	需要购买一定数量的群控设备，设备成本较高。
■ 流量挂机	流量来源于全国各地，源IP为真实用户IP。	刷量效率依赖于挂机平台用户数量和挂机软件安装量。
■ 多开模式	多开模式刷量主要为通过视频窗口多开，达到刷量目的。此模式相对来说，技术难度及成本较低。	刷量速度相对较慢。
■ 人工刷量	完全真实用户，无法通过技术手段检测。	派单结算流程较为繁琐，且依赖于自有会员资源，上量速度较慢且成本相对较高，仅适用于对播放量有效性有明确要求的客户。

2.6. 刷量特征与反欺诈策略

根据主流视频平台与刷量团伙的攻防对抗，我们总结出以下刷量特征：

平台检测维度	刷量团伙对抗策略
▪ 用户 ID	利用接码平台、打码平台、注册机等大量注册平台小号； 购买大量会员账号； 租用共享账号。
▪ IP	通过代理 IP、秒拨机等设备，不断切换 IP。
▪ 设备指纹	通过硬改软件修改手机设备指纹； 通过模拟器伪造设备信息。
▪ 缓存	通过清除缓存或使用无痕模式，再次观看，算作新增播放量。
▪ 浏览行为	部分平台打开视频网页即算作一次播放量，可通过按键精灵等模拟点击工具反复开关网页提高播放量。
▪ 高相关度卡段播放量	播放视频内容高相关片段。
▪ 播放行为特征	模拟视频真实播放量增长曲线，如播放量与时间粘度。

视频平台与刷量黑灰产的攻防对抗一直存在，以下为威胁猎人建议的反欺诈策略：

 通过监测访问用户、终端、IP 等信息，建立用户、终端、IP 等多维黑名单库，只有通过过滤的播放记录才会记入最终的有效流量。	 在用户行为层面，从多个维度对用户的行为进行分析，建立用户行为特征库，并对异常播放行为进行过滤。	 建立多维监控系统，紧跟黑产不断升级的作弊手段，能够及时发现异常播放数据，补充异常流量特征。	 与第三方安全公司、公安部门合作，从司法层面主动打击作弊团伙。
--	--	--	---

3. 在线视频流量欺诈黑灰产团伙分析

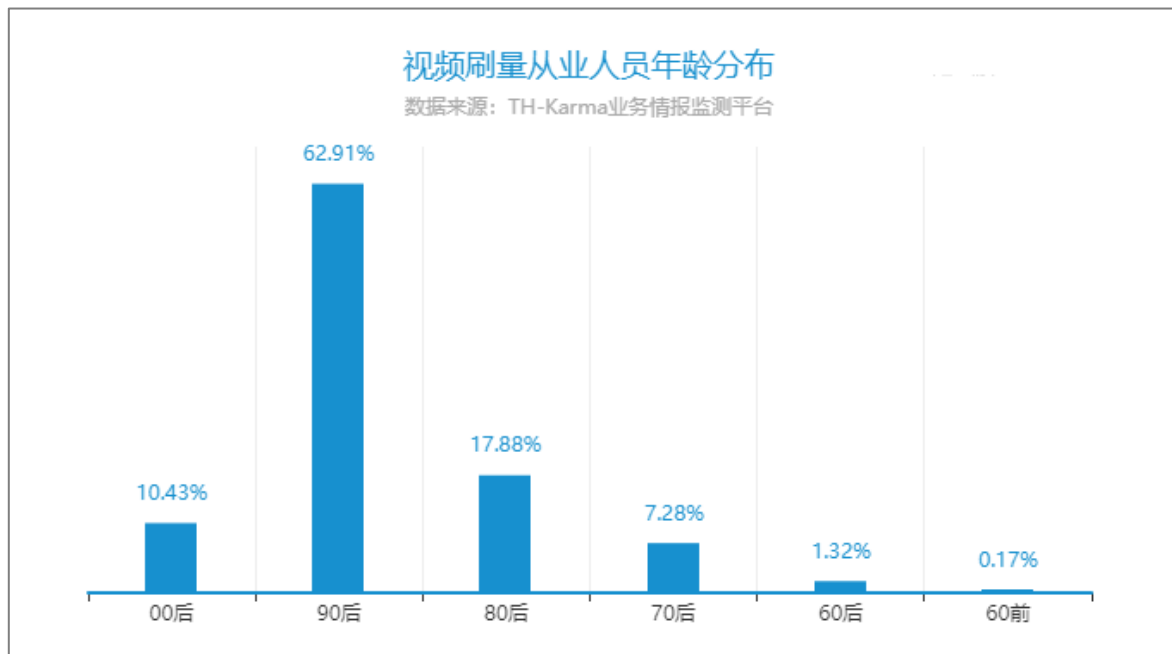
3.1. 刷量黑灰产人员群体数据

3.1.1. 规模大小

威胁猎人通过长期监测视频刷量黑灰产业务，接触视频刷量相关群体，并主动接洽了多个大型的刷量团伙和工作室，了解到某大型工作室每月维护服务器和囤买账号的费用高达百万以上，但很快可以回本，推测目前从事视频刷量的黑灰产从业人员数十万人，年产值数十亿元。

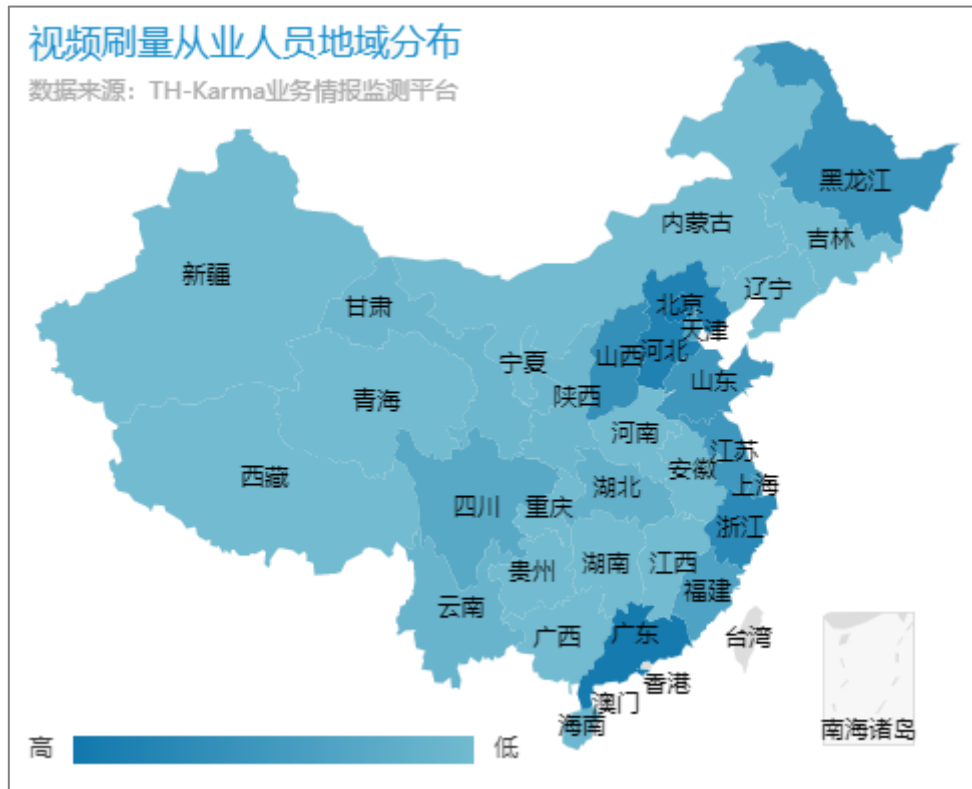
3.1.2. 年龄层次

从年龄分布来看，刷量从业人员主要集中在 90 后，占据从业人员比例超过 60%。90 后不仅作为当代消费的主力军，同样成为当代黑灰产业的主力军。作为较早一批接触互联网的 80 后，在黑灰产中也占据了将近 20% 的比例。详情如下图所示：



3.1.3. 地域分布

下图展示了刷量从业人员的地域分布情况。可以发现，刷量从业人员集中于我国的东部地区，其中北京、广东、河北、浙江、山西占据了地域分布榜单前五名，基本符合经济发展水平和人口密集度分布。由此可见，越是经济发达的地区，互联网犯罪越是多发，相对而言经济欠发达的地区，利用互联网犯罪还未形成规模。详情如下图所示：





3.2. 多为工作室形式

刷量从业人员多数以工作室形式存在，工作室成员分工明确，有自己的技术团队、运营团队、销售团队等，工作室成员人数根据公司业务范畴在几十人甚至上百人不等。

我们以某工作室为例，该工作室详细展示了自身的团队成员结构：

业务团队	成员结构				
	项目总监	前期沟通	策划	文案	执行汇总
知 (12人)	(1人)	(3人)	(3人)	(3人)	(2人)
豆 (9人)	(1人)	(3人)	(1人)	(2人)	(2人)
小红书 (11人)	(1人)	(3人)	(2人)	(2人)	(3人)
(13人)	(1人)	(3人)	(3人)	(3人)	(3人)
(10人)	(1人)	(3人)	(2人)	(2人)	(2人)
其他 (19人)	(1人)	(5人)	(5人)	(4人)	(4人)

3.3. 业务种类多样化

从事在线视频刷量的工作室团伙，往往并不只进行单一的业务，涉及的业务领域众多，比如微博、新闻网站、公众号、客户端、小红书、抖音等其他推广业务，甚至可以承接国外市场推广。业务范围具有明显的趋利性，如今大热的短视频和直播行业、美妆类 App 等，是黑灰产工作室重点推广的业务线。以下为某工作室团伙可以承接的业务举例：

业务	描述
新闻网站、软文推广	覆盖全国各行业上万家媒体。
客户端首页智能推荐	智能推荐 600 元，阅读 10 万+，提供后台数据。
微信公众号	覆盖全网各种行业的微信公众号。
KPI 数据维护	视频网站、微博、微信、弹幕、转发、评论、赞等。
小红书	小红书 KOL 美妆母婴达人、素人、网红，原创笔记、视频、上热门。
视频首页推广	各大视频网站首页推广(爱奇艺、搜狐视频、乐视视频、腾讯视频、bilibili、AcFun 等)。
抖音	抖音网红号，报价实时更新。
知乎	知乎、KOL、数据维护、问答、点赞、评论。
微博热门话题榜、热搜	流量最集中的话题榜、微博热搜，专业团队运作。
豆瓣	豆瓣并分、上分、KOL。

某 P2P 流量挂机平台可承接的业务举例：



3.4. 技术更新快

专业的刷量从业者可以说对视频网站的风控细节了如指掌，比如某视频平台一周内会调整几次参数、多久重置数据等，除了平台安全团队本身，刷量团伙可能是最为关注平台风控策略的群体。刷量黑灰产人员通常是团队作战，并且拥有自主研发的技术和平台，可以及时应对平台更新的风控策略，研究出新的刷量算法。

以针对某视频平台的一款注册机工具来看，该工具一直有版本迭代更新，更新频率最高可以达到一天 5 个版本，每一次更新就意味着黑灰产与平台之间的一次对抗博弈：

MD5	文件名	首次发现时间
e686aa1f978c386f56a9d30a4d2f839c	【刘米其】邀请注册v1.81-爱00.exe	2018/12/3 21:30
6df28de6db7a03192403ad15e3da9269	【刘米其】邀请注册v1.8- exe	2018/12/3 0:32
7b6780a0c22233b0e8f8855fd45ab209	【刘米其】邀请注册v1.781- .exe	2018/12/3 0:01
73e18f35f09df1632e07bdf1a23b0ee2	【刘米其】邀请注册v1.771- .exe	2018/12/2 21:33
c63e758af22a0d5aabaf15f9d21716f8	【刘米其】邀请注册v1.77- .exe	2018/12/2 20:30
0d04bdeca5249f8b29e85a2086cde323	【刘米其】邀请注册v1.76- .exe	2018/12/2 20:05
717f5fe9231a315215aba7e5ab8eb711	【刘米其】邀请注册v1.75- .exe	2018/12/2 19:14
57474a1794abc84098cb054ec466d2f7	【刘米其】邀请注册v1.75- .exe	2018/12/2 19:09
78a8e1459d4c45c3bb16e9bc466d9e5b	【刘米其】邀请注册v1.75- .exe	2018/12/2 19:04
f49dd7b8908c4b69c4fdb2b65aa91b11	【刘米其】邀请注册v1.73- .exe	2018/12/2 17:11
90704e71f31daa66e773d619575a6255	【刘米其】邀请注册v1.73- .exe	2018/12/2 17:09

3.5. 游走在灰色地带

与电信诈骗、非法贩卖公民信息等具有明确违法犯罪的性质不同的是，刷量一直游走在法律的灰色边缘地带。部分从事广告推广、市场营销、公关活动等正常业务的工作室，也会承接刷量业务，并且刷量业务被包装为所谓的视频数据维护业务，并且工作室有正规的注册信息和网站，部分工作室还能提供合同与正规发票。例如，下图为某视频刷量工作室官网展示的业务范围及介绍：

 公关活动 我们为您提供企业年会、周年庆典、会议论坛、团建拓展、开业庆典及酒会宴会等公关活动的策划与执行，实现卓有成效的公关效果。	 数字营销 我们的资深数字营销顾问为您提供超过30万KOL微博、微信公众号、今日头条及抖音等新媒体平台的丰富资源整合与精准营销传播。	 声誉管理 我们帮助全球在华机构提供CSR企业社会责任的策略规划与活动执行，基于亿级大数据舆情监测系统实现危机公关管理与快速处置。
 演艺经纪 我们拥有丰富的主持人、歌手、演员、乐队及模特资源，提供魔术、杂技、沙画、武术、川剧变脸、舞狮、相声及戏曲等商业演出服务。	 会议会展 我们为您提供演唱会、研讨会、高峰论坛、国际会议、展博会、演讲会、学术会及招商会的策划、场馆、搭建及招商的全流程会务服务。	 媒体关系 我们为中国、美国、日本、韩国、俄罗斯、菲律宾等中外广告商及行业客户提供全球超过七千家优质新闻媒介资源，提升新闻传播效果。

其中的数字营销业务，就涉及到视频刷量等灰色业务：

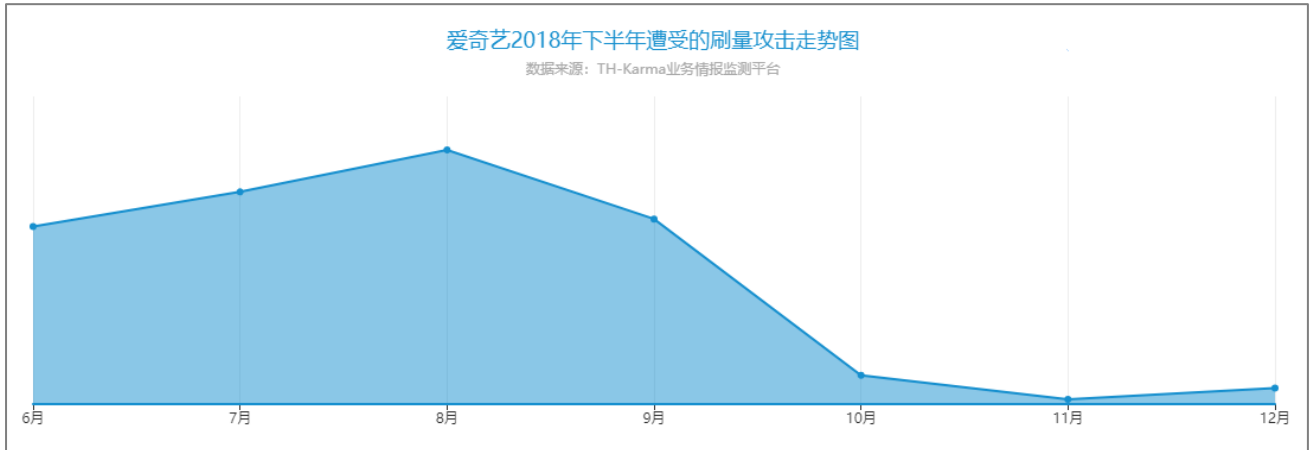
数字营销项目	业务描述
■ 视频流量	视频网站流量数据维护，安全、稳定、高效。
■ 知乎推广	机构号运营，话题冲榜，热点发酵传播。
■ 豆瓣推广	影视剧专业影评，推广，讨论区维护。
■ 小红书推广	用转化率和服务说话，淘宝天猫商家必备。

4. 写在最后

流量战争中，视频刷量究竟动了谁的奶酪？

报告一开始就指出，不论是对视频平台，广告主，还是制片方，从长远角度看，都是受害者。整场视频流量的博弈中，刷量黑灰产从业者或许是唯一的受益方。然而在现阶段，由于种种原因，有的群体想与刷量黑灰产对抗，但受限于资源、能力的限制，“有心无力”；另一方面，有的群体却为了短期私利，破坏市场竞争环境，对刷量行为视而不见，甚至在幕后推波助澜，助长黑灰产的气焰。

可喜的是，已经有在线视频平台率先并持续性与视频刷量黑灰产进行着积极地对抗，并且效果显著。下图为爱奇艺 2018 年下半年遭受的视频刷量攻击走势图，随着该平台在 2018 年 9 月份上线包括关闭前台播放量展示的新策略，刷量攻击曾一度出现断崖式下跌：



但是，少数平台的积极对抗并不能给视频刷量黑灰产予以重创，还需整个行业联手，共同净化市场环境。

从整个互联网内容行业的角度来说，刷量都是必须要清除的害群之马。互联网内容行业如何健康持续性发展，有赖于内容展示平台、内容提供方、广告商以及用户等利益相关体之间长久的相互关注与信任。威胁猎人作为一家专业的第三方黑灰产情报研究机构，也会继续关注刷量产业链的发展与变化，并与各方共同努力，为互联网内容行业营造一个健康干净的市场环境。

说 明

1. 关于业务情报监测平台 TH-Karma:

业务情报监测平台 TH-Karma，依托威胁猎人对黑灰产实时布控的能力输出的业务情报监测平台，采用多维度的数据收集和深层次的情报处理体系，为企业提供最及时有效的全景式业务风险感知能力，帮助企业在早期就能发现业务风险并量化对业务的影响，持续对黑产进行多维度监控，做好企业的业务风险侦察兵。

2. 关于威胁猎人:

威胁猎人是一家以业务安全情报能力见长的创新型安全企业，旨在为客户提供业务攻防情报，从防控到打击的全方位业务安全解决方案。自成立始，公司投入大量资源，打造了一整套国内领先的业务安全情报监控与预警体系，形成强大的黑灰产布控能力，为客户提供黑灰产情报及业务风控解决方案。目前已为腾讯、百度、阿里、华为等近百家全国 TOP 级互联网企业提供服务。

3. 联系方式:

商务合作: th-business@threathunter.cn

转载授权: th-marketing@threathunter.cn

公司官网: www.threathunter.cn

联系电话: 0755-2660 0293

公司地址: 广东省深圳市南山区科华路讯美科技广场 3 栋 15 层 K 室



欢迎关注威胁猎人公众号，获取更多专业报告