黑镜调查

深渊背后的真相之

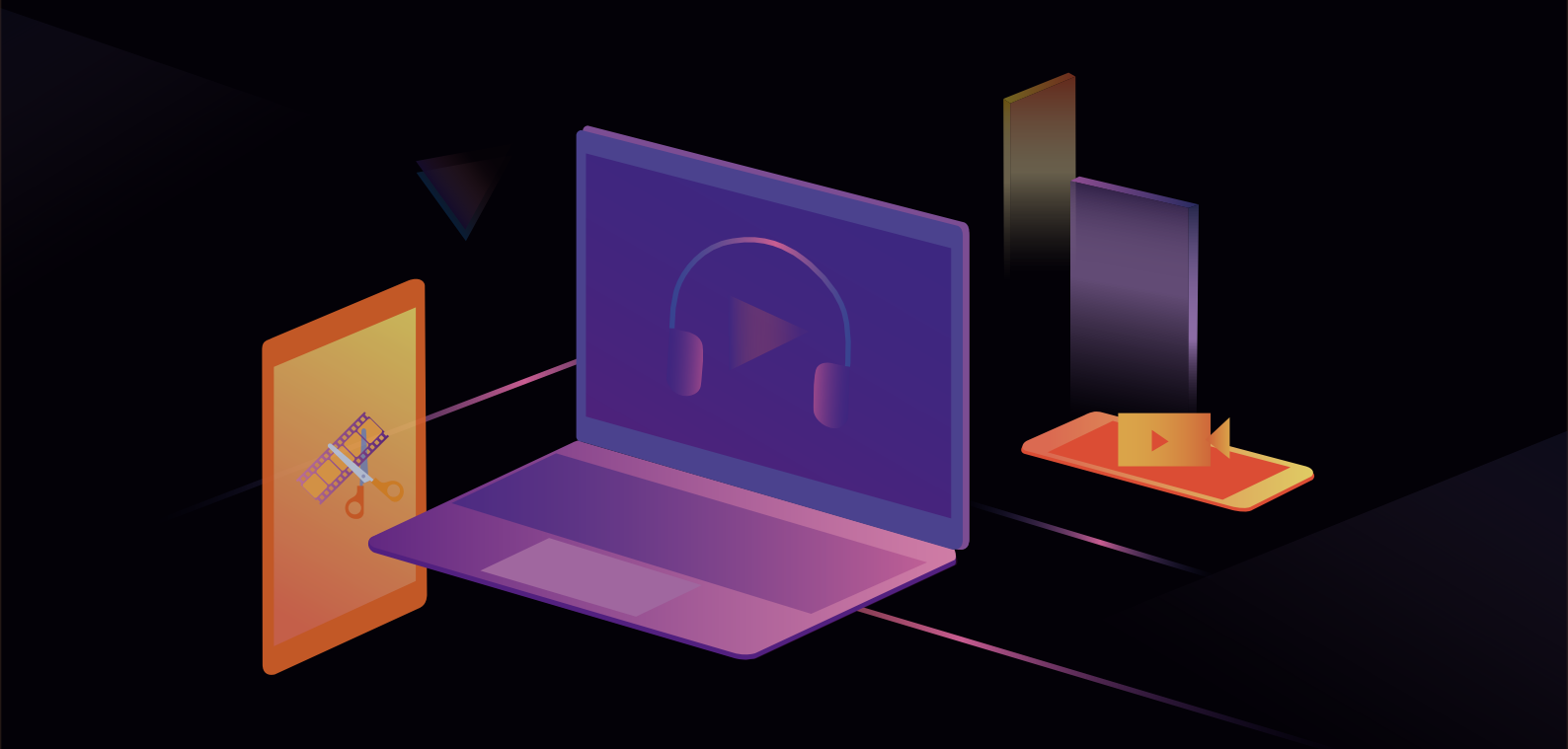
「短视频黑灰产业」报告

FREEBUF 威胁猎人 THREAT HUNTER

声明

本报告为FreeBuf与威胁猎人联合研究成果。报告中所涉及的数据来自网上公开数据，或采取合法技术手段、深度调查、抽样调查等方式获取。由于统计方法不同、视角和数据观察维度不同，与市场实情可能存在一定误差。此外，报告中所涉及的人名均为化名。

本文仅从学术角度做分析研究，任何非法行为都将受到法律严惩。



关于 FreeBuf 研究院

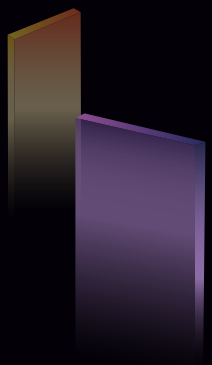
FreeBuf.COM 是斗象科技旗下、国内领先的互联网安全新媒体，每日发布最专业的安全资讯、技术剖析，分享国内外最新安全资源，是最受安全从业者与爱好者关注的网络安全网站与社区。FreeBuf研究院则集结了行业内经验丰富的安全专家和分析师，常年对信息安全技术、行业动态保持追踪，呈现最专业的安全行业现状和趋势分析。

关于威胁猎人

威胁猎人是国内最专业的业务安全威胁情报服务商。威胁猎人于2017年推出了多款业务安全情报产品，专注于为互联网业务安全领域的游戏、电商、消费金融、政企、O2O等诸多互联网细分市场，提供安全可靠的威胁情报服务；可帮助互联网公司更好的完善安全攻防闭环，增强未知风险感知、量化已知风险，并通过情报工具直接提升整体业务安全能力。目前威胁猎人已为国内众多一线知名互联网企业提供安全保护服务，致力让安全从业者更了解黑灰产业链，帮助互联网厂商从攻击者视角搭建业务安全纵深防御体系。

数据及内容支持

TH-KARMA业务安全情报平台　　漏洞盒子



目录

第四章 短视频行业黑灰产团伙画像

第五章 应对方法与安全建议

第一章 概述

1.1 内容简介

“双击666”、“老铁没毛病”、“快点答题开始了”、“吃到鸡了”……从2017年到2018年，以上说辞纷纷成为网络热词，也成为许多网民的口头禅。从最早风靡微博的秒拍，到现在的短视频一哥快手；从“2016年第一网红”papi酱到现在抖音上的各大戏精用户，短视频行业在2017年迎来了大爆发，也引发了新一轮流量大狂欢。各大厂商纷纷入局，短视频APP层出不穷，很难说用户是被这一轮狂欢挟裹而前，还是这些用户促成了短视频行业的烈火烹油之势。准确来说，网民与网络，相辅相成，相互造就了如今的互联网江湖。

QuestMobile发布的《2017年中国移动互联网年度报告》显示，2017年短视频行业月活跃用户规模持续增长，与2016年同期相比增长率达116.5%，截至2017年12月，短视频独立APP行业用户已经达到惊人的4.14亿[1]。CNNIC发布的第41 次《中国互联网络发展状况统计报告》显示，2016年12月到2017年12月，我国网民对网络视频的使用率达到75%，对手机网络视频的使用率达到72.9%[2]。此外，在 2017年底突然风靡起来的直播答题，又为短视频行业找到了新的突破口。全民答题，热闹非凡，仿佛再现了当年央视颇受欢迎的“幸运 52 ”场面。

不论是怀旧还是追新，不论是早早下场胸有成竹，还是匆匆闯入顺势而为，都验证了互联网各种活动不变的主题：流量与变现。而依赖互联网生存的黑灰产，也从不会放过任何一个可以谋利的机会。流量抢夺和积累是变现的开始。短视频行业聚集了大把流量，随着其飞速的发展，与此相关的地下产业链也逐渐形成了工具化、自动化、团伙化、规模化的长期盈利模式，按照环节有序攫取利润。

作为黑产系列报告的第二部，本报告从“短视频黑灰产业链”入手，通过对短视频及直播答题行业浅析，结合威胁猎人TH-Karma情报中心的数十亿级情报数据以及十几个短视频、直播答题相关的QQ群调查结果，利用数据分析、真实调查等方式，揭秘伴随短视频和直播答题应运而生的黑灰产业链详情，以期为读者呈现短视频黑灰产业链画像。此外，报告中的真实案例也体现出企业运营过程中出现的技术或业务疏漏，提醒企业、项目管理者重视产品和业务中的安全问题。同时，也借此为相关决策者提供一定的参考和指导。

1.2 重要发现

- 近一年短视频和直播答题的大火也相应地带动了短视频黑灰产的发展；目前短视频黑灰产已经群体化、规模化，形成了完整的产业链；
- 2017年，短视频平台月平均遭受攻击20亿次左右，团伙行为极度疯狂；
- 短视频黑灰产下游环节中，引流相关的团伙数量最多，体现黑灰产“流量为王”的特点；
- 直播答题平台近一月遭遇的最高攻击达200万以上；24小时攻击量变化与答题时间密切相关；
- 短视频攻击IP遍布全国十几个省、市、地区，相关QQ群数量庞大，广东、山东、河南等成为较大的IP来源地和QQ群分布地；
- 短视频黑灰产利用到语音识别、OCR识别、自动化工具甚至人工智能神经网络等多种技术；涉及账号买卖、社工、诈骗、刷流量等多个环节；
- QQ群、微信群、淘宝等社群或平台成为国内短视频黑灰产扩张的根据地；
- 企业需加强防范意识，使用合适的安全产品和安全服务；
- 监管部门应当加大执法力度和普法力度，从上游打击黑灰产，并提升全民网络安全意识；

第二章 短视频行业浅析

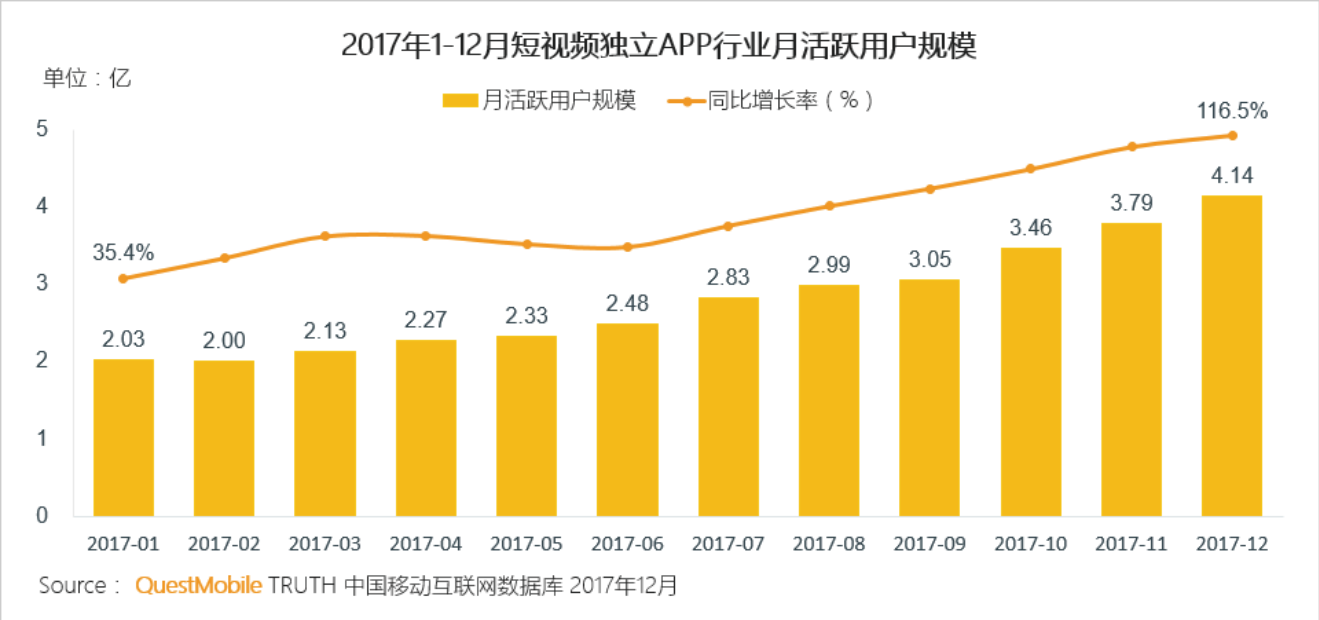
短视频被视为新媒体时代，内容创业的下一个风口。近年来，互联网用户兴趣重心逐渐从传统的图文内容转移到短视频，尤其是在“2016年第一网红”papi酱凭借趣味短视频爆红之后，更多人看到了行业潜力，间接推动了短视频行业的疯狂增长。

由于具备门槛低、自我表达、易于传播的特性，普通用户也可以运用碎片时间创作、分享和交流，因此短视频吸引了越来越多的用户以及资本力量进入。2017年，短视频行业迎来大爆发。除了BAT之外，还有后起之秀如今日头条等巨头企业以直接或者间接的身份参与到这场不断涌现新玩法的产业中。

2.1 短视频行业

短视频，顾名思义是时长较短的视频。包括在朋友圈常见的10s以下小视频，也包括类似电影预告这种几分钟长度的宣传片或者网络上传播的各种趣味视频。短视频兴起之初，原本并没有准确的时间限制，但根据各大短视频平台对于视频时长的限制，再加上适合广泛传播的短视频经验判断，因此业内对于短视频达成了以下共识：

短视频即短片视频，是一种互联网内容传播方式，一般指在互联网新媒体上传播、时长在5分钟以内的视频传播内容[3]。

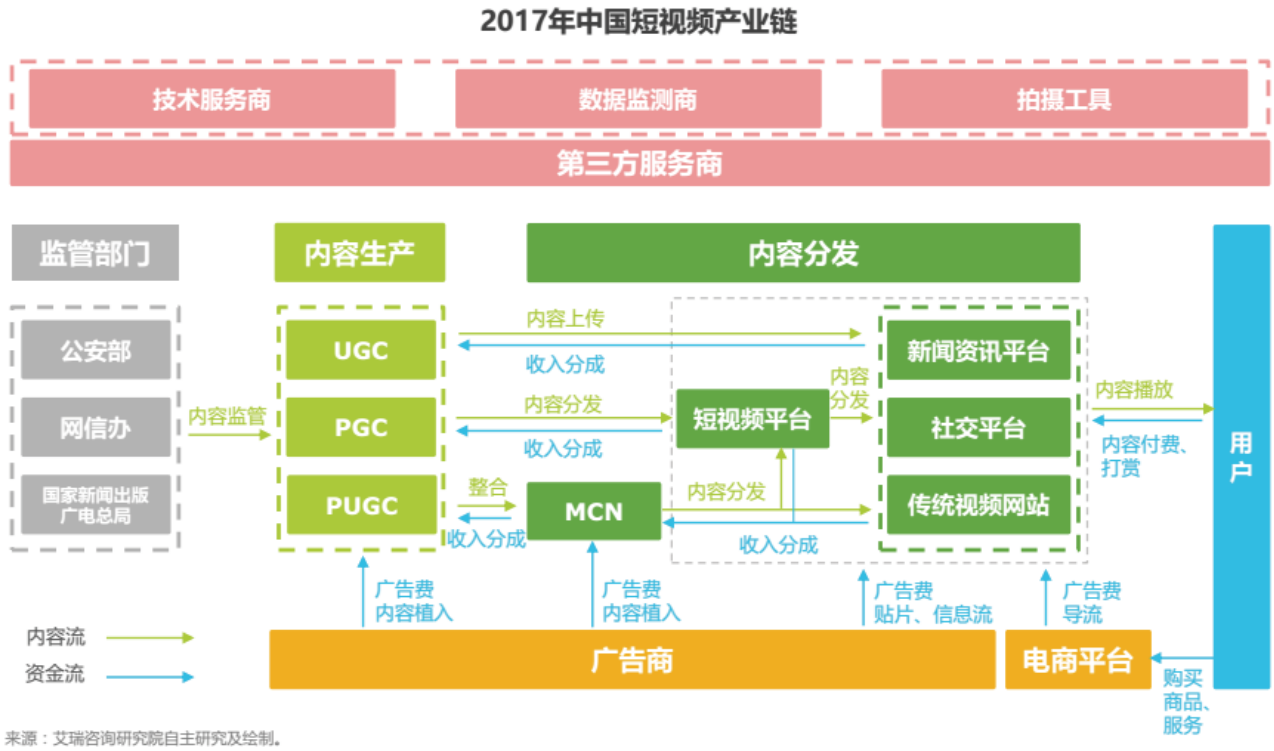


根据QuestMobile发布的《2017年中国移动互联网年度报告》，2017年短视频行业月活跃用户规模持续增长，年增长率达116.5%。截至2017年底短视频活跃用户规模已经达到惊人的4.14亿。其中，快手以超过2亿的月活跃用户规模成为短视频行业NO.1[1]。

除此之外，还有一些值得关注的短视频平台增长势头不容小觑，如西瓜视频、抖音、火山小视频、秒拍、美拍以及梨视频。不过，亲身体验一番，也能发现这些平台存在一定的区别。其中，抖音、火山小视频专注于传播15秒短视频，即用户发布的视频时长不超过15秒。火山小视频并没有鲜明的用户区分，而抖音大多以音乐短视频为主。相比之下，其他平台对于市场和视频类别并没有特别严格的限制。

可以说短视频行业的发展模式是分别借鉴了直播平台以及新媒体资讯平台，短视频平台本身并不产出内容，依靠UGC（用户生产内容）和PGC（专业生产内容）来保持平台内容的稳定更新。

而UGC和PGC两种模式下最大的区别就是专业性，大部分普通用户并没有足够的专业技能去制作高品质短视频，远不及专业内容团队。也因此导致普通用户想成为“网红”相对更难，而平台本身也更加注重PGC内容或者一小部分网红的产出，来提升平台竞争力。



艾瑞咨询:2017中国短视频行业研究报告[4]

为了鼓励更优质的内容产出，短视频平台也给予了一定的奖励措施，类似自媒体平台的分成奖励，同时借鉴直播平台的打赏模式来刺激内容产出方积极的运营能力。而平台本身大多依靠广告和用户打赏抽成来盈利。

由于短视频平台大大依赖于粉丝运营和流量分成，且平台运营者为了竞争也投入大量补贴和奖励，最终催生了针对短视频平台的刷粉、刷流量甚至薅羊毛（运营垃圾号）

的黑灰产业链。

平台	背景	MAU	估值	变现模式	黑产利用环节
快手	腾讯、百度投资	2.04 亿	180 亿美元	广告、用户付费	刷粉、刷流量及垃圾号
西瓜视频	原头条视频	8206 万		广告、用户付费	刷粉、刷流量及垃圾号
火山小视频	今日头条内部孵化	7790 万		广告、用户付费	刷粉、刷流量及垃圾号
抖音		5548 万		广告、用户付费	刷粉、刷流量
秒拍	新浪微博官方短视频应用			广告、用户付费	刷粉、刷流量
美拍	短视频界美图秀秀			广告、用户付费	刷粉、刷流量
梨视频	资讯短视频平台			广告、用户付费	刷粉、刷流量及垃圾号

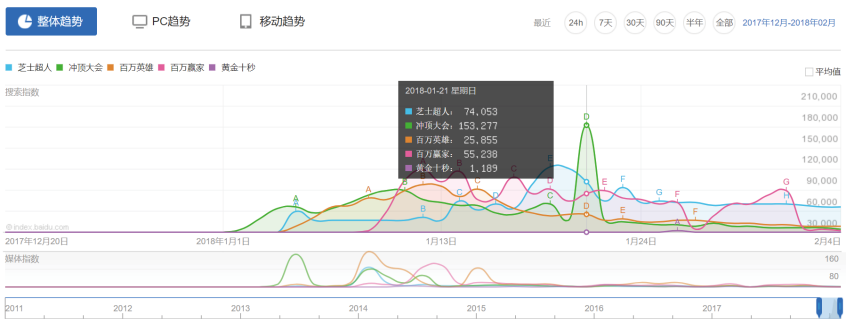
短视频代表平台一览 **FreeBuf 研究院自主研究制作**

2.2 直播答题

2018年一到，王思聪、周鸿祎等大佬相继“撒币”，冲顶大会、百万英雄、芝士超人等直播答题平台扎堆上线，活脱脱网络版的“开心辞典”，并很快吸引了数百万活跃用户，甚至人民日报都发文点赞称“正能量也能带流量”。从初期的质疑到全民参与的火热局面，直播答题也带动了短视频平台及其背后的资本角逐，让短视频平台迎来新的爆点。

虽然每个平台每天只在几个准点开放答题，但一次10万的奖金却能吸引到50万甚至一百万的高活跃用户参与，这笔生意看起来势头大好。相继出现的广告甚至远远超过在短视频平台或者直播平台的广告效果，也让人看到了这种盈利方式的超高回报率。

而这种直播答题的入口除了上线单独的APP之外，还会在直播平台或者短视频平台设立入口，一来迅速拉动活跃用户，二来可以将直播答题的用户间接引入到短视频、直播平台上，可谓一举两得。直播答题平台由最开始的五六家增涨至目前的二三十家，并且还不断有新玩家加入。



近一个月各直播答题平台百度搜索指数 [5]

答对12道题就能瓜分几百万的大奖，这相比当初支付宝集齐“五福”的活动诱惑力和可参与度大的多了。五福卡尚且可以在淘宝买到，如此火爆的直播答题活动又怎能不让黑产眼红呢？

名称	关联平台	入场时间	站台大咖	单场最高奖金池	历史最高单人奖金	答题时段（时间安排非固定）	黑产利用环节
芝士超人	映客直播	2017.12.24	朱啸虎、汪涵、谢娜	202万	101万	12：30、19：30、20：30、21：30、22：30	刷复活币、售卖题库、售卖答题辅助软件、线上建群
冲顶大会	冲顶大会	2017.12.26	王思聪、叫兽易小星	30万	5100元	13：00、17：00、19：00、21：00	
百万英雄	西瓜视频	2018.01.03	张一鸣、王凯、柳岩	305万	4万+	13：00、20：00、21：00、22：00、23：00	
百万赢家	花椒直播	2018.01.05	周鸿祎、李好	388万	103万	12：30、13：30、16：30到22：30每小时一场	
黄金十秒	一直播	2018.01.10	韩坤、张绍刚	200万	95元	12：30、15：30、17：30、20：30	

直播答题代表平台一览　　FreeBuf 研究院自主研究制作

第三章 短视频黑灰产业链

3.1 产业链概述

基于上述对短视频行业的分析，刷粉、刷量、工具软件销售等与短视频平台相关的牟利方式已经形成了环环相扣的产业链。根据需求，服务一应俱全，从账号商人、工具开发者到代理IP平台、手机卡商、接码平台等，每一层都有成熟的利润获取方式。

与短视频平台直接相关的盈利行为有三种：搬运工薅羊毛、刷量作弊以及引流变现。

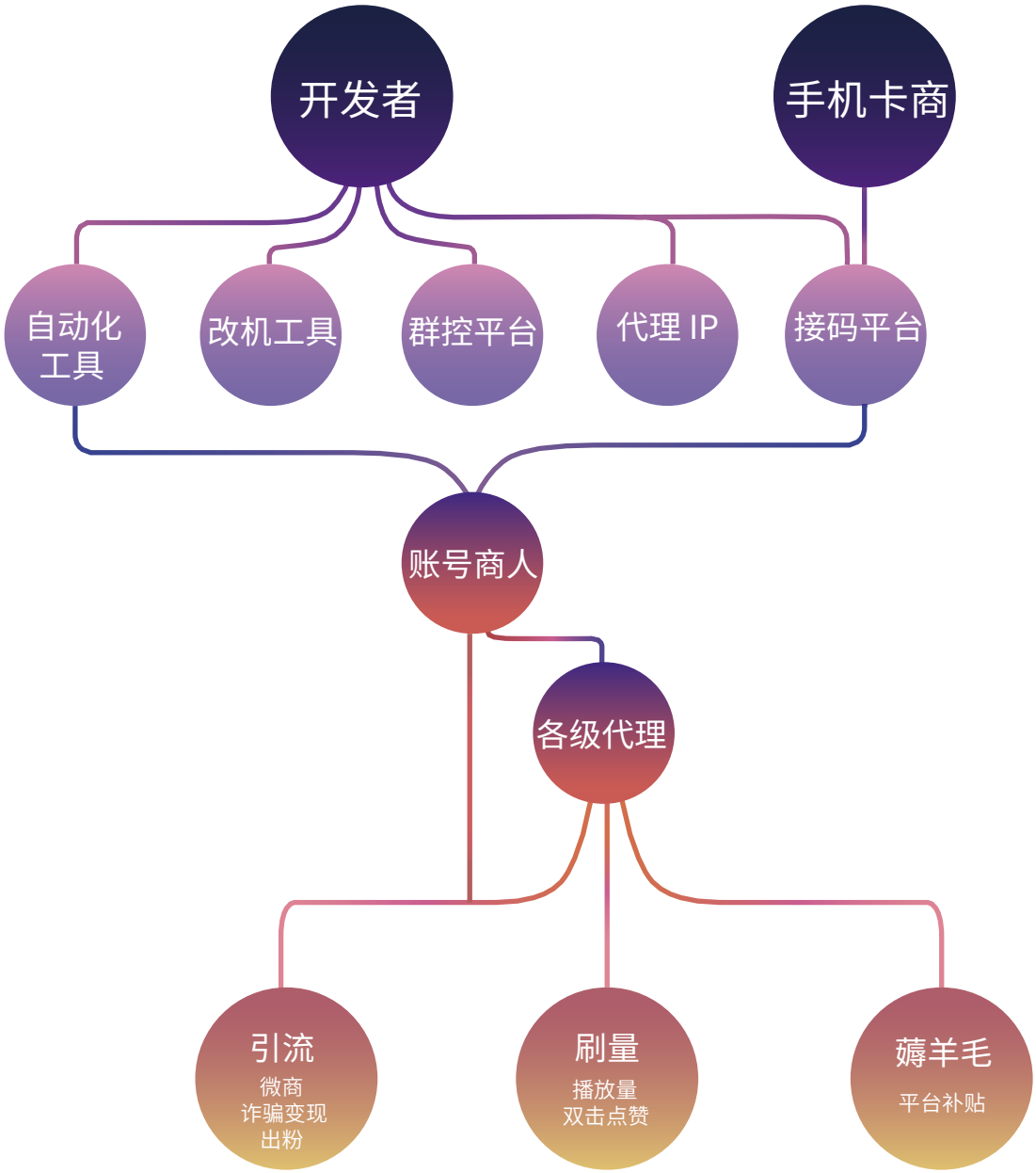
- **搬运工薅羊毛**：例如，当平台有补贴等鼓励活动时，采集其它平台优质视频，修改上传；有时搭配作弊冲击平台的各项指标，骗取现金奖励。

- **刷量作弊**：刷粉、刷点赞、刷播放量等数据赚取现金。

- **引流变现**：将短视频平台的用户（目标消费群体），引至微信等处，再以微商、诈骗等方式深度变现，多数为微商。以下用微信代指引流变现出口。

这三种盈利方式都处于整个产业链的最下游，而上游的开发者、卡商、代理等，其实与“薅羊毛”产业链中的上游环节基本相同，这也间接反映了黑灰产业链上游高度重合的情况。

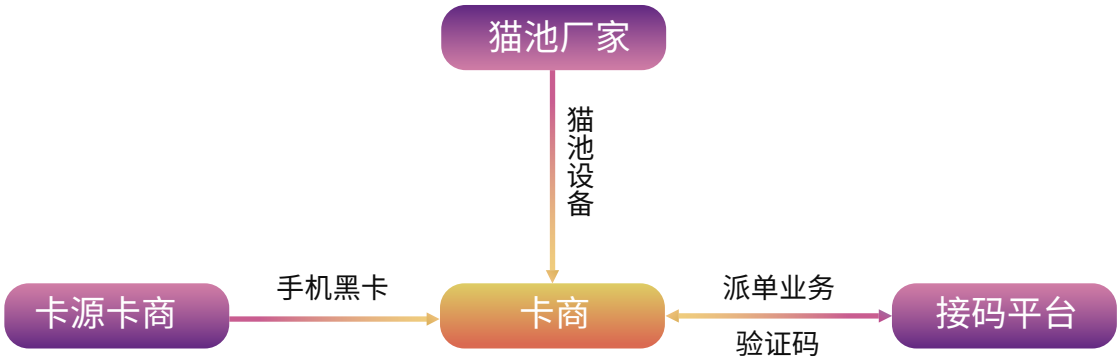
整体短视频相关产业链的结构，大致如下，以下将一一介绍。



短视频黑灰产产业链图

3.2 手机卡商

手机卡商，能够为接码平台和黑灰产从业者提供大量手机号，用以各种虚假注册、认证业务。这些手机卡我们称其为黑卡，黑卡产业的背后产业链大概如下图所示：



黑卡产业链

3.2.1 卡源卡商

卡源卡商通过各种渠道（如：开皮包公司、与代理商打通关系等）从运营商或代理商那里办理大量的手机卡，然后加价转卖给下游卡商赚取差价，他们掌握着手机黑卡货源。

根据反向追踪调查，卡源主要有：

物联网卡：无须实名认证，主要用于工业、交通、物流等领域。物联网卡需要以企业名义办理，卡商以千元左右的价格可轻易购得“营业执照”进行办理，且一张营业执照几乎对办理数量不做限制。这种卡多为0月租（或1月租），根据能否接听电话，分为

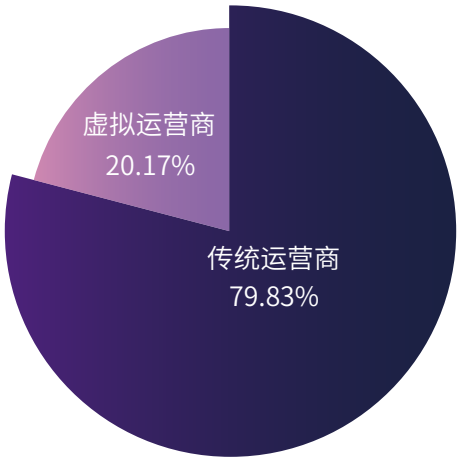
短信卡（也称注册卡，只能收短信，给1069打头的服务号发短信）和语音卡（用以接收语音验证码和发送验证短信等业务）。有些运营商甚至会为灰产定制专用的物联网卡套餐。

实名卡：这种卡多为联络运营商后，从网上收集大量身份证信息批量认证得来。

海外卡：由于实名制的原因，16年下半年开始，大量缅甸、越南、印尼等东南亚卡开始进入国内手机黑卡产业。这些卡支持GSM网络，国内可直接使用，无需实名认证，基本是0月租，收短信免费，非常切合黑产利益。

威胁猎人维护着多维度分析的恶意手机号码库，根据号码库数据进行分析得到如下结论。

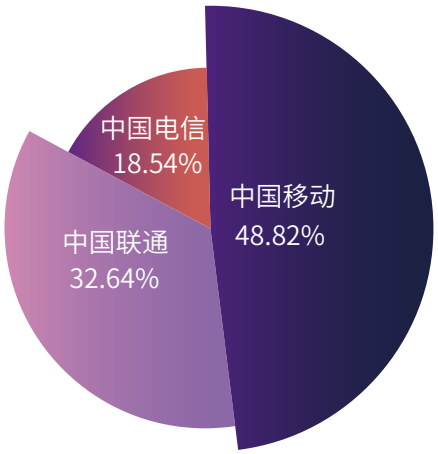
a）手机黑卡运营商对比



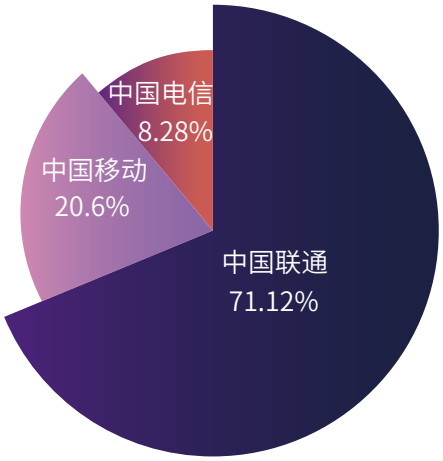
传统运营商和虚拟运营商黑卡数量对比

来自传统运营商的黑卡数量要远多于来自虚拟运营商的黑卡数量，毕竟传统运营商和虚拟运营商的手机卡总量不在同一个数量级上。2017年8月份的新闻数据表明，全国虚拟运营商用户占移动用户总数的3.6%，3.6%的用户占比却贡献了20.17%的黑卡数量占比，说明相对传统运营商而言，虚拟运营商的手机卡中黑卡占比较高。

以下两张图展示了在非虚拟号段上和虚拟号段上三大运营商的黑卡数量对比：



非虚拟号段

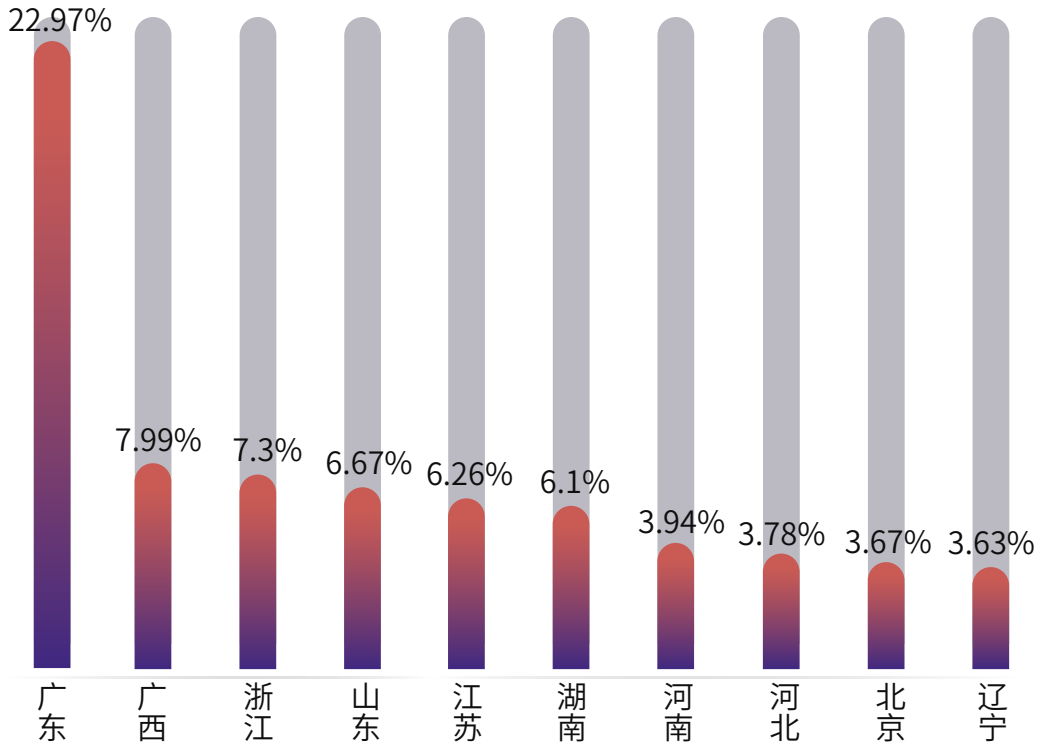


虚拟号段

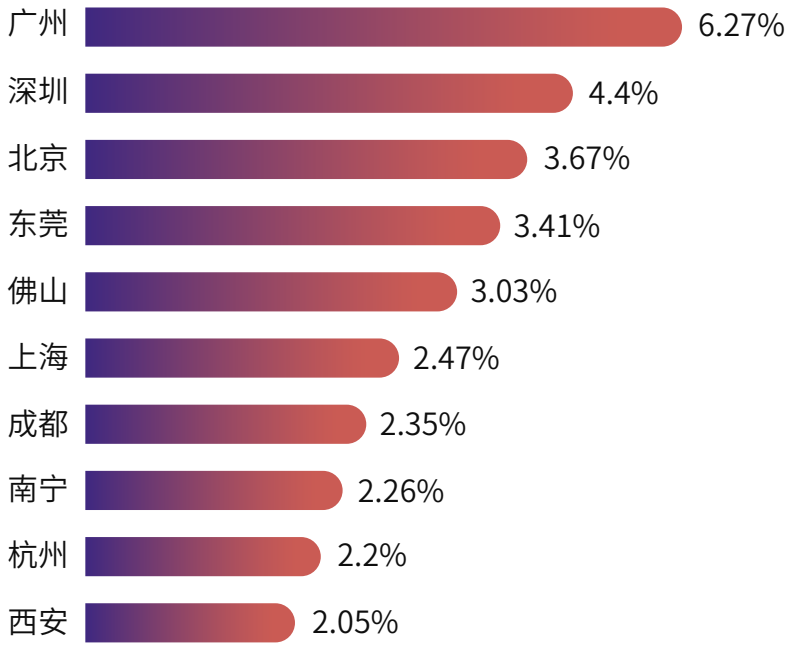
在非虚拟号段上，将近一半的手机黑卡来自于中国移动，约三分之一来自中国联通，中国电信最少。在虚拟号段上，绝大多数是中国联通的手机黑卡，中国移动次之，中国电信依旧最少。

b）手机黑卡归属地分布

以下是依据黑卡归属地统计的数据，广东省十分抢眼，在黑卡归属地省份排名中遥遥领先，省内的广州、深圳、东莞和佛山也在黑卡归属地城市中名列前茅。



黑卡归属地国内省份top 10



黑卡归属地国内城市top 10

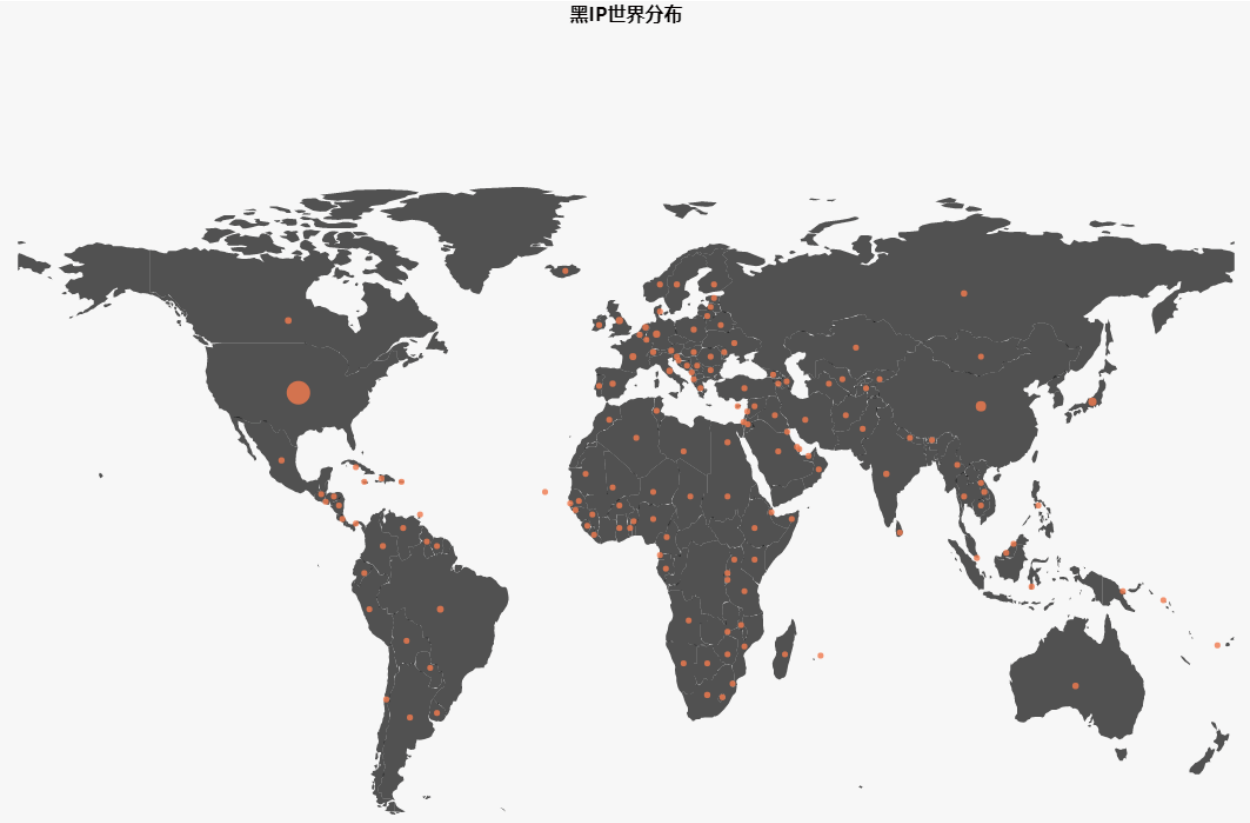
3.2.2 猫池厂家

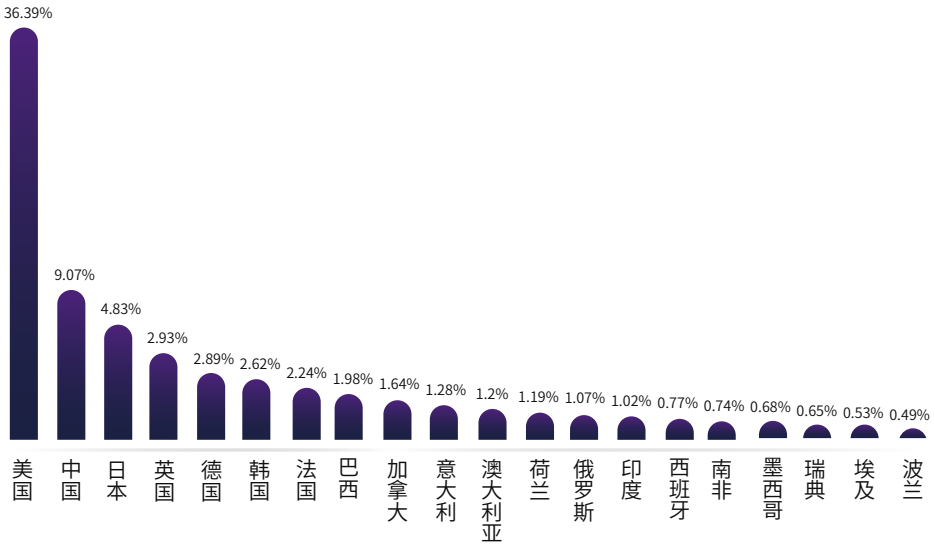
猫池厂家负责生产猫池设备，并将设备卖给卡商使用。猫池是一种插上手机卡就可以模拟手机进行收发短信、接打电话、上网等功能的设备，在正常行业也有广泛应用，如邮电局、银行、证券商、各类交易所、各类信息呼叫中心等。猫池设备可以实现对多张手机卡的管理。

3.3 代理IP

用于网络攻击的IP，即黑IP。黑灰产从业者为了隐藏自己的真实IP，同时也为了绕过甲方的IP风控策略，需要大量的IP资源（比如代理IP）作为跳板，进而发动网络攻击。威胁猎人通过大量渠道收集信息，做了详细分类。

分析IP地域来源数据，全球黑IP分布图和top 20来源国家如下：

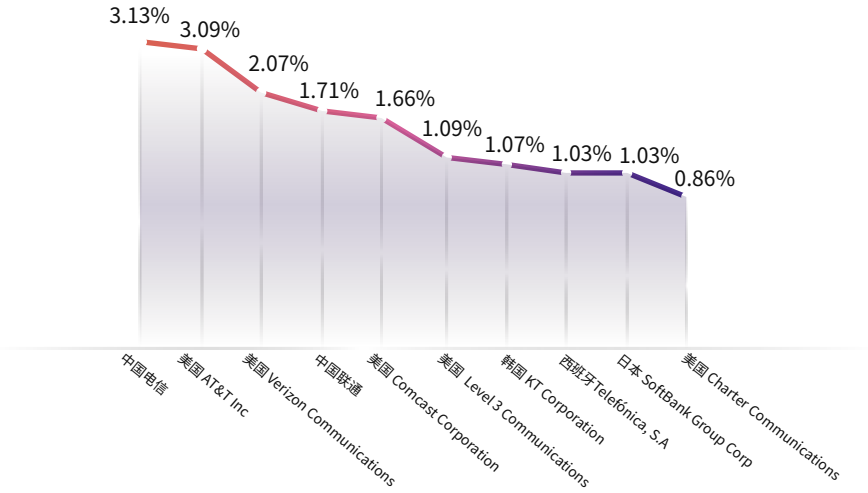




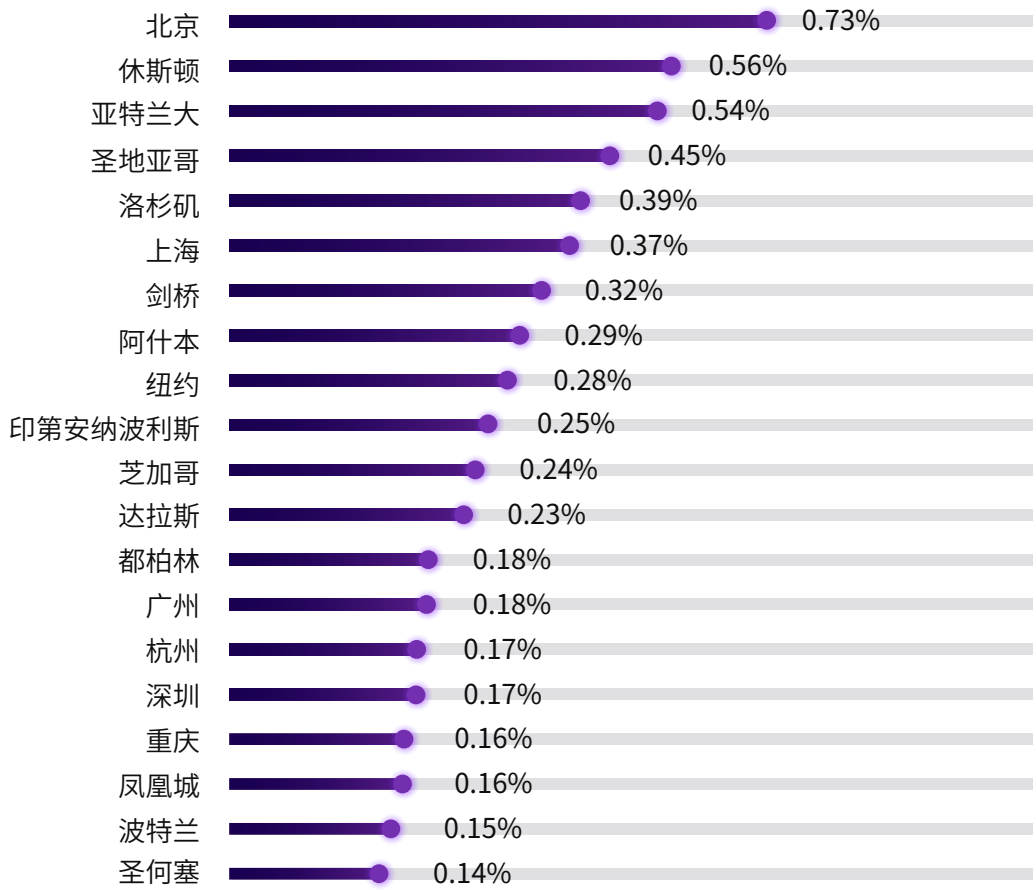
全球黑IP来源国家top 20

全球IPv4总数约为43亿，美国拥有30%以上，这一数据与上图相符，美国的黑IP数量占比36.39%，遥遥领先其他国家。发达国家的黑IP数量要多于发展中国家，可以简单理解为，发达国家拥有更多的互联网设备，也就拥有更多的IP资源，所以黑IP的数量与互联网设备的数量成正比。

以下两张图片为全球黑IP所属运营商top 10和全球黑IP来源城市top 20：



全球黑IP所属运营商top 10



全球黑IP来源城市top 20

从来源城市数据看来，top榜单中大多数是美国城市，中国城市数量紧随其后，其中北京更是占据了榜首。上榜的城市都是经济较为发达的城市。从所属运营商数据看来，top10中一半是美国的运营商。

3.4 接码平台

接码平台负责连接卡商和羊毛党、号商等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。接码平台很多，活跃的有数十家，比较知名的有：Thewolf、星辰、爱乐赞、玉米（现“菜众享”）等，其中Thewolf和星辰可以接语音验证码。2016年11月，当时最大的平台爱码被警方查处，随后很多平台转入地下。

平台一般会提供客户端和API接口，接口可以用来对接自动化的工具。根据使用项目的不同（如一些项目只需要识别短信中的验证码，一些却需要发送短信进行验证），平台会合理安排手机卡的使用，用户也可以选择在平台上对接专属卡商，既能节省成本，又能提高自己使用黑卡的质量。

3.5 羊毛党/号商/代理

当某个平台做营销活动时，羊毛党就会出动，大批量注册账号参与活动获取奖励。

号商则是大量注册并养各个平台的账号，通过出售账号获利。这些账号可以用于引流、刷量等后续业务。

代理则是通过网站、论坛、QQ群等多个渠道分发账号等资源，相当于黑中介。

根据平台登录方式和账号种类，号码商一般销售三种账号：手机直登、跳转号、带某些属性的账号（如一定等级、特定权限等）。

- **手机直登**：用手机号直接注册的号码。
- **跳转号**：采用第三方平台登录的方式，将其它平台的小号转换成短视频平台账号。
- **属性号**：盗号、扫号、养号等方式获得的账号。

直登和跳转号多是使用群控系统、注册机等自动化工具批量注册。带属性的账号多为盗号等方式获得。以下将逐一介绍。

3.5.1 群控系统

群控系统的使用是为了避过平台对设备的检测。即采用电脑来控制多部移动设备，如下图为针对iPhone的群控系统，能够让连接的多部手机根据既定脚本批量执行操作。对于账号注册部分，系统集合了过滑动验证、自动获取填写验证码、修改资料等功能。

群控系统操作界面

每台设备会存在注册账号数量的限制，这时会结合改机软件来解决。改机软件通过劫持系统函数，修改UDID、IMEI、SSID、定位等设备信息的，使平台检测认为是新的手机。

上述平台结合了NZT一键新机工具，该工具除了修改设备信息，还提供一键新机、多开、全息备份等功能。只对勾选的app更新设备参数，能够导出参数备份信息，为跨机共享和恢复某账号设备环境提供便利。

使用群控系统时，每部手机都会安装触动精灵，它会按照既定的Lua脚本去执行触摸，滑动，输入文本等操作，使用者可以根据不同目的找开发人定制专门的脚本。

群控系统、触动精灵和改机工具结合使用，再接入接码平台和代理IP，就可以高效的产出质量过硬的号码。这种方式完全模仿真实用户，较难分辨。厂商可以从“虚假号码”、黑IP、用户行为及进入app后的操作顺序等角度着手判断。

接码平台上的项目数量和单价，可以侧面体现平台账号批量注册的严重程度以及绕过手机号验证的成本。

接码平台项目截图

3.5.2 注册机

注册机多是自动化批量注册的工具，多是采用易语言进行开发，在Windows下运行，技术手法有两种：

- **模拟操作类**：通过控件操作浏览器元素实现，真实加载注册页面，模拟用户操作。
- **协议破解类**：通过HTTPS协议实现，破解注册接口协议，直接带参数调用注册接口实现注册。

手机号资源自然是从接码平台获取，IP资源使用ADSL拨号（使用VPS挂机操作等），这背后也有一条完整的产业链支撑。大多注册机的速度可达到几十秒注册一个账号，为下游的各个细分产业提供大量的小号。

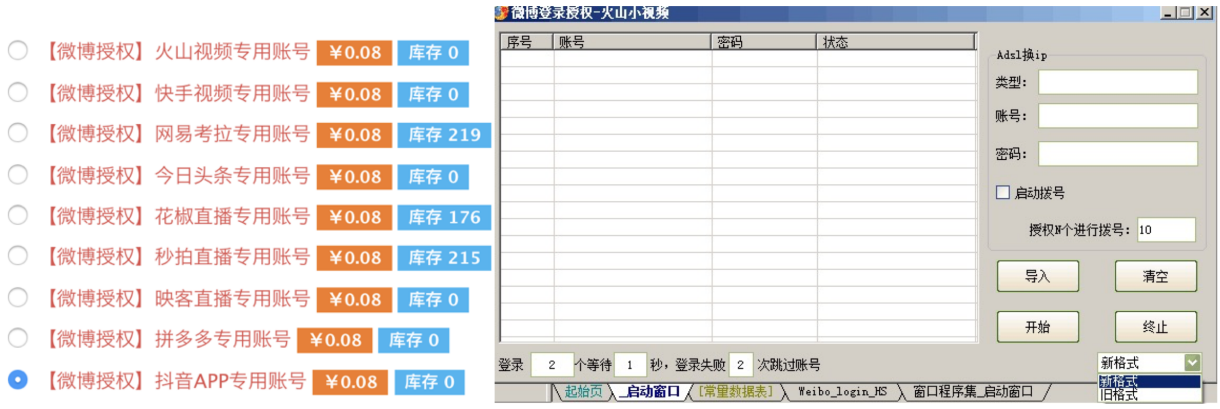
有些平台的策略会对这类账号造成影响，即有些注册机出来的号码，几天内会失效，但仍可以对接“直接用量怼的项目”，一般会采用预定方式售卖账号，随买随用。

美拍注册机

3.5.3 跳转号

除了直登号外，跳转号也是常见的号码。指使用QQ号或者微博快捷登录后，激活绑定而转化而成的平台账号。这里使用的QQ和微博号并非正常账号，而是称为授权号的特殊账号，这种账号在原有平台（QQ和微博）质量很低，无法进行大部分业务。所以只用作授权其他平台，购买成本仅几分钱。

如图2-4和接码平台类似，为了充分利用和不重复使用，也会根据要授权的平台进行分类，右侧为授权软件，可批量将微博小号转为火山账号。



微博授权号和火山授权软件

如上所述，在互联网灰产领域，账号注册已经形成了有人去专业操作的事情。许多工作室依赖注册和贩卖各种账号生存，这些账号已经成为了具有广泛销量的基础资源，再流入各个细分产业链。小号虽小，却要在风控战场上引起大的重视。

3.5.4 盗号、扫号和养号

老号指有一定注册时间、自身带有权重的号码，有的还带有一定的粉丝与作品。这类号码被认为不易封号，在市场上受欢迎。老号和带有一定权限等级的号码，一般是采用这三种方式得到的：

- **盗号**：主要方式是钓鱼，如发布二次打包的软件——将某些软件打包加入自己需要的功能，当用户使用这些动过手脚的软件时，黑客就会收到他们的账户名、密码 。
- **扫号**：方法有两种：1、用接码平台的手机号作为用户名，遇到注册过的直接修改密码，这种属于黑吃黑，拿走了别人批量注册的号码。2、使用其他手段获取大量账号名，加上弱密码，去逐一验证，这种账号是真实用户，对平台伤害较大。
- **养号**：号商注册后模仿真实用户进行一些操作，将号码养老的行为。大多是为了提高账号的权重，以方便之后的项目。平台伤害较大。

3.6 引流变现

一个简单的引流变现操作是这样的：操作者在头像、昵称、个人资料等地方留下微信号，再使用各种方式增加曝光度，从而使更多的用户前往添加微信，之后使用微信进行深度变现。以下介绍短视频平台上几个常见的方法。

3.6.1 同城视频的利用

在同城界面，距离我们越近的人，他的视频就会被排在越靠前的位置。这一点被利用形成了一种引流方式——“出0.1播放量”。

如前文提到的改机工具NZT，也提供虚拟定位功能，利用此功能，可以使定位点十几公里内的人，看到该视频的距离都是0.1km，从而让视频排长久霸占在置顶的位置上。

用这种方式，可以在短时间内，快速获得一定的播放量，有时在有一定播放量后，平台还会助力推广，使得播放量上涨更快，进而提高成功引流的人数。

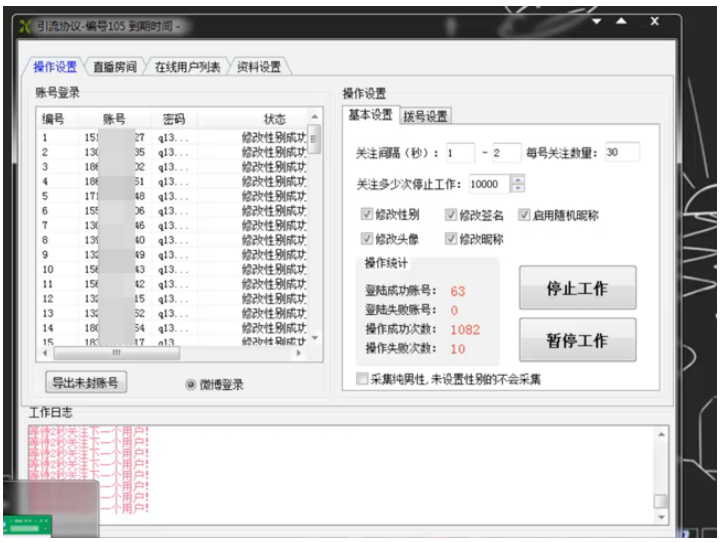
多数利用播放量的引流方式都会参考相应平台的推广策略。

3.6.2 评论、直播引流等

评论引流即在特定热门视频下评论吸引用户，有时会配合刷量，将其刷成热门评论。如图软件会自动筛选新的视频（比较活跃）和直播人数高的直播间评论指定内容。

某推广助手

直播引流有很多方法，如在直播间挂入小号批量评论。也有利用工具转播其他平台的直播，收取礼物提现，顺便使用资料曝光微信号引流。如下图一款火山视频引流软件的做法是：自动将小号修改性别（女），然后批量关注直播间的用户（吸引注意），在配合签名中的诱惑性的话语，邀请用户加微信好友。有的软件还配备筛选功能，如只关注刷了礼物的“大户”，向他们发送私信等。



引流协议

引流方法非常之多，仔细观察，他们目的明确，创意十足，十分清楚自己的需要引流的目标群体。如下图利用参与评论的用户，软件可以筛选，在某一视频下评论过的用户，逐一发送私信（与当前视频话题紧密相关的内容）。当引流操作人想到新的方式，测试有效，就会立刻去找开发人定制工具投入使用。

美拍私信推广助手

3.6.3 群控系统和模拟器

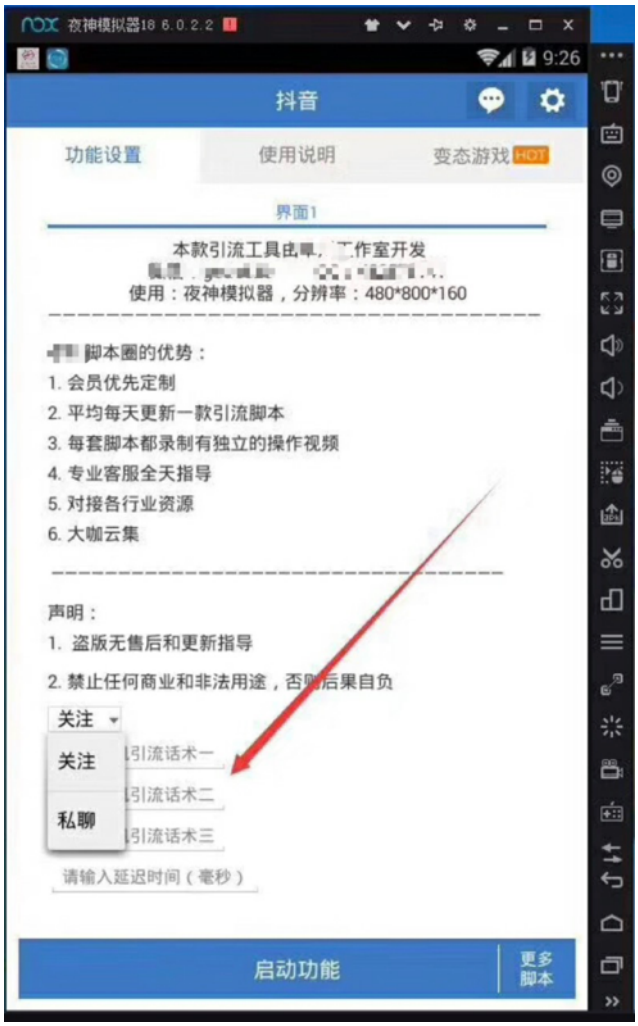
上文提到的群控系统自然也可以引流，操作者也可以使用群控自动上传作品。

有些短视频平台检测到账号资料有留下微信号，封面话语露骨时，会认为有引流意图，进行封号或屏蔽该账号的视频。群控系统还可以通过加入监控解决这个问题：先上传视频，当有一定播放量以后，认为通过了平台检测，及时通知操作者更改资料进行引流。

除了使用真机，也有很多人使用模拟器达到目的，有些模拟器也增加了一些改机功能，操作简单，刷新或重启动后就是另外一套参数。安卓模拟器较为常见，引流和搬运薅羊毛多是使用模拟器进行。

如下图，一个是使用模拟器薅直播答题的羊毛，一个是配合模拟器的抖音引流脚本。

直播答题薅羊毛成功截图


夜神模拟器18 6.0.2.2
9:26
抖音
功能设置
使用说明
变态游戏 HOT
界面1
本款引流工具由[redacted]工作室开发
使用：夜神模拟器，分辨率：480*800*160
[redacted]脚本圈的优势：
1. 会员优先定制
2. 平均每天更新一款引流脚本
3. 每套脚本都录制有独立的操作视频
4. 专业客服全天指导
5. 对接各行业资源
6. 大咖云集
声明：
1. 盗版无售后和更新指导
2. 禁止任何商业和非法用途，否则后果自负
关注
关注
私聊
引流话术一
引流话术二
引流话术三
请输入延迟时间（毫秒）
启动功能
更多脚本

抖音引流脚本

3.6.4 出粉

一些数量的引流操作，可以带来非常巨大的流量，个人无法消耗，会以“出粉”形式卖出，即买家按照成功加微信的“人头”数，付给引流者报酬。

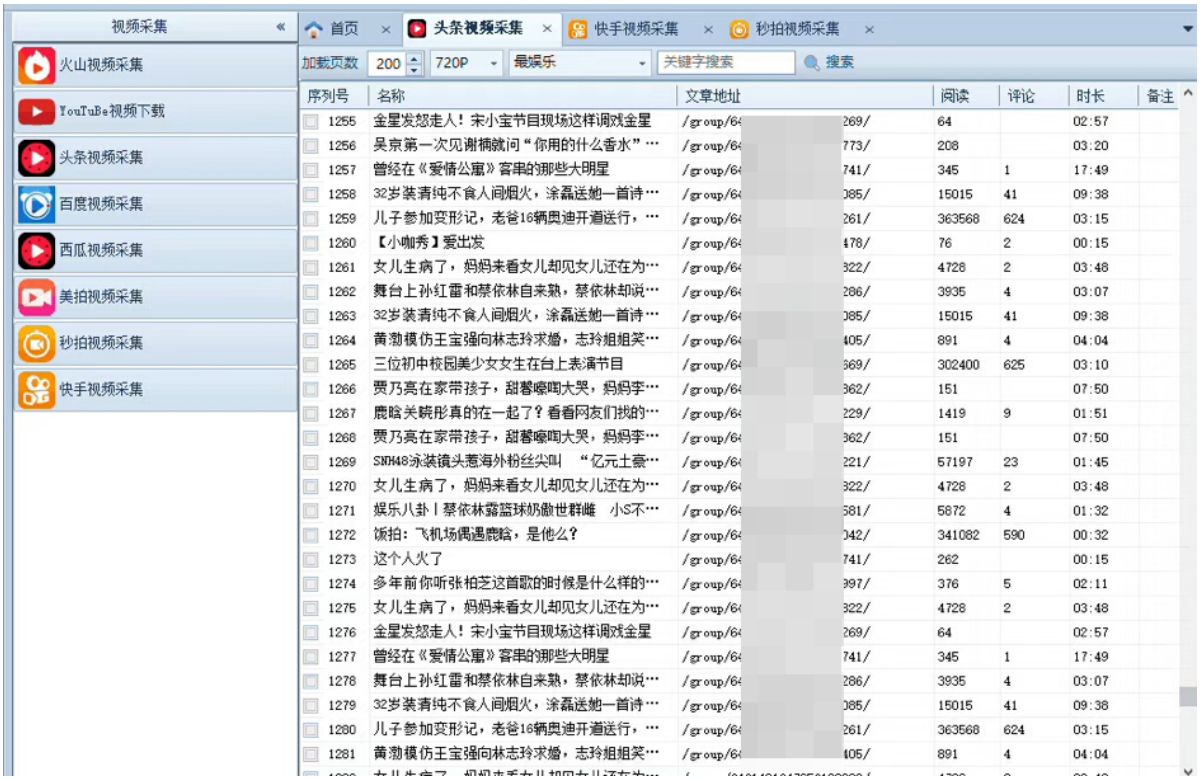
操作人会结合“话术”提高成功率，如吸引“女粉”，会写“前100人免费送XXX化妆水”，吸引“男粉”，会在美女视频的封面上添加“想找男朋友”等，此种方案称为“封面话术”。

根据客户的不同，引流操作会选择不同的视频，美女视频来的叫做“色粉”、“男粉”，会进一步在微信中骗取红包或者销售一些男性用品。美妆视频引来的“女粉”，卖给销售化妆品的微商。诸如此类，还有销售假货、医疗用品、保健品的“粉”。

3.7 视频采集

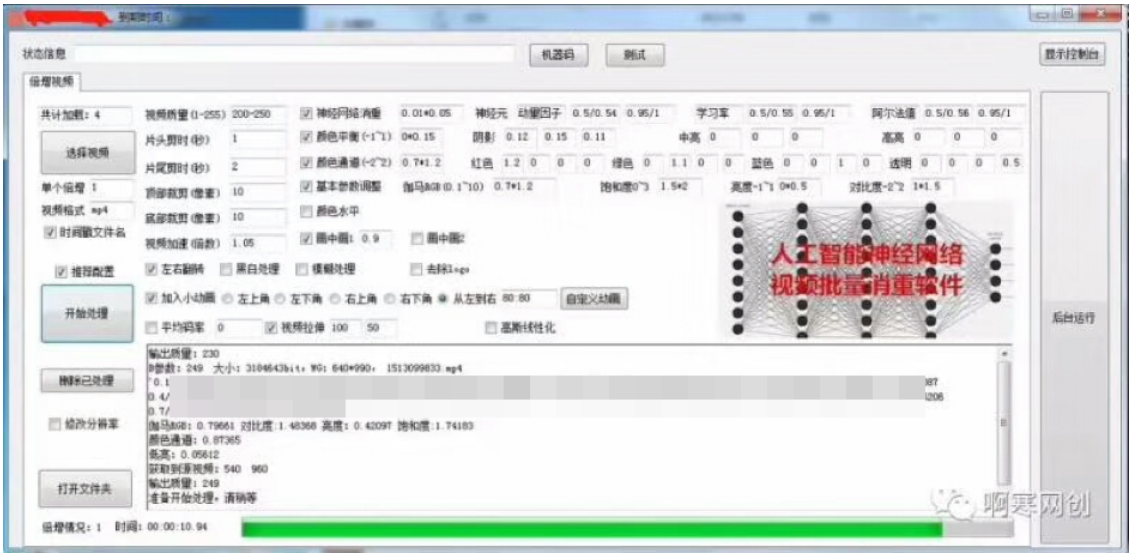
通过视频播放量等方法的引流，对视频需求量很大，于是市场上有非常多的采集网站和采集软件。这些软件可以解析出视频的真实地址，达到无水印下载的目的。

黑灰产也遵循需求产生产品的原则，薅羊毛小团伙和个人，往往会使用解析网站单个下载视频。而引流需要批量化操作，为了给引流提供便利，很多软件都会具备批量和筛选功能，如下载某个人的全部视频、他喜欢的全部视频，进而下载同一类视频，引流相应目标用户。如下图为一个集合型的工具，能够下载大部分短视频平台的视频。



视频采集器

采集视频后，操作人还会使用相关的工具软件对视频批量修改，使其能够通过平台的原创检测，如下图为一修改消重工具，声称利用了人工智能神经网络技术。



视频消重工具

开发者也会互相售卖算法、源码等，其他开发者购买后再集成“顾客”的其他需求，最终输出定制软件。

算法源码出售截图

提高排名、吸引粉丝、接广告要达到标准等等，刷量的需求很大，方式也有很多。市场上常见的一种方法是破解通信协议，当然以上提到的工具大多都可以进行上来刷量。

关于视频类的有很多“XX协议”，这些就是指利用通信协议达到目的的软件。 先扫出小号的参数：token、cookie等，在用这些参数批量去访问固定的接口，达到欺骗目的，实现刷量。

如下图，导入cookie后，可以刷视频评论、点赞、播放量以及用户粉丝。

刷量协议

第四章 短视频行业黑灰产团伙画像

4.1 短视频黑灰产团伙

4.1.1 行为分析

面对短视频平台的火热，被黑产利用的套路除了常见的刷粉、刷流量之外，连简单的视频后期包装也被搬上了某宝产业链。

刷粉	播放量	评价	喜欢	转发
100粉丝=10元	1000播放=2元	1条=0.5元	1喜欢=0.1元	待定
1000粉丝=90元	5000播放=10元	10条=5元	10喜欢=1元	
5000粉丝=400元	1万播放=20元	20条=10元	100喜欢=9元	
1万粉丝=700元	2万播放=35元	100条=45元	1000喜欢=80元	

在搜索引擎找到某刷粉平台，可以看到，刷粉、刷播放量、刷评论以及点赞甚至转发都能够明码标价进行交易，甚至还有专门的刷粉软件出售。

除此之外，为了获取平台更多的分成，已经涌现出不少运营大量垃圾号的个人或者团队，在部分短视频平台依靠个性化推送，一些劣质内容很容易就混进去。这些垃圾号发布的内容基本是靠搬运+简单剪辑，只求量而不求质的内容。利用标题以及带有诱惑性封面来骗取更多的流量，基于流量数据，平台也提供可观的奖励。这种现象在自媒体平台以及部分短视频平台都比较普遍，也带动了短视频平台账号及相关软件的买卖服务。平台的风控策略越严，运营时间越久，平台用户质量越高，价格就会越高。

小号	价格
快手	¥4.00
火山	¥0.30
抖音	¥0.20
陌陌（满月）	¥5.00
美拍	¥2.00

引流软件		视频上传	
美拍私信推广	300	趣多拍视频上传	199/月
火山直播引流	199/月	头条视频上传	200/月

刷量软件	业务	注册机	价格
火山 399元	视频点赞、评论、刷播放量、关注用户	头条	¥100.00
小咖秀 499元	视频点赞、视频评论、关注用户	火山	¥100.00
抖音 599元	视频点赞、评论、刷播放量、关注用户	美拍	¥90.00

大部分的薅羊毛和引流，都是个人和小团伙在操作，大不过一个小型工作室。不过正如我们上一份《薅羊毛产业报告》所言，这些团伙常常聚集在QQ群和微信群，集体行动、传播消息，一些群主能够积累数量庞大的下线。

群主会先放出薅羊毛项目或引流方法吸引人们加群，再通过微信、Q群和“圈子”放出自己的付费群号码，收费从百元到千元不等。付费群可以获取质量好盈利高的项目、分享最新的自动化工具、甚至提供各种黑灰产相关的技术和服务。

收费群推广与活动

如此一来群主解决了自己人手不够，盈利值保持在瓶颈无法突破的问题，也利用“新情报”为自己制造了额外创收。但同时，作为受害者的平台却被迅速薅走活动经费，同时因为引流和搬运薅羊毛都需要上传视频，而充斥了大量伪原创视频和虚假用户信息，对日后的用户行为、用户特征分析造成了极大的干扰。

这些攻击方式简单，工具也谈不上包含了多高的技术。但架不住人数的冲击，团伙化、产业化的行动模式仍然会对平台造成规模化的伤害。

有一定人手的工作室都不会依赖于某一个平台，如大多数的账号商人会销售几个不同平台的账号，规避风险，同时还做一定量的引流业务出粉等。除此之外，号商、引流者、开发者等还会以师傅带徒弟，徒弟出师再带徒弟的方式赚取利润。这样一来，一个攻击方法产生，积累了适宜的变现能力后，规模就会迅速扩大，各路人马层层蚕食利润，直到平台做出限制，黑产重新寻找新的方法。

当一个平台策略提升后，短期内因为平台的相似性，操作者会大量流往其他平台。然而竞争者少了，饼的大小却没有变化，会有人不断测试，找出新的绕过方法。一段时间后，少数人掌握的技术，逐渐变成大家都知道的规则，操作者流回，循环往复。而平台会持续的面临问题：平台推广需要提防羊毛党，账号增加价值要保证账号安全，视频作品要解决引流对原创性的打击等等。

4.1.2 团伙缩影——S君与短视频平台

广东省的S君和妻子小美，共同经营着一家小商品行，除了贩卖商品有很多的空闲时间。在接触了不少网赚项目后，逐渐有了自己的“业务”，目前主要是做号和销售A短视频平台的各种账号。

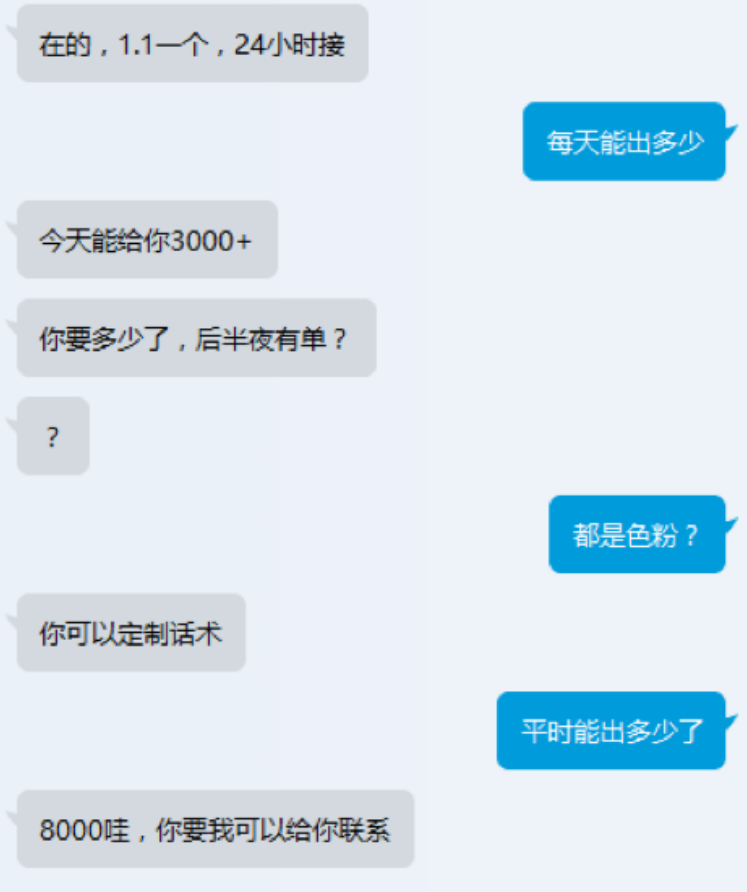
A平台刚实施了一次严厉打击，当平台认为某个号码存在被盗号的风险，就会要求验证手机号。在以前，这个平台最好用的是“老号”，大家都是拿扫号工具扫出来的。现在有八成需要验证，同时，做项目时，封号率变得越来越高,账号价格飙升。

S和自己的“技术人员”经过几番测试后，放弃了扫号。“A平台变严了，盗的号没原来好用了，用我的方法批量注册的新号引流都能过，扫号现在没什么做的意思了，用过就知道了。”S的注册引流方法是群控，用真机加脚本的方式出号、自动发视频作品，会判断是否通过平台的检测，通过后才进行引流，没有就进行养号操作。

因为引流效果好，S的号在市场上十分受欢迎。S每天至少出六七千个号，每个号赚小两块钱。原来出号的时候，估摸着顾客要多少，做多了的就提高一块钱价格，挂在自动发货平台上当零售卖。现在可顾不上更新平台了，老顾客每天要的都做不出来了。

“每天都要出号到三点，才能不误了老客户的事儿。卡商真是不给力，动不动就没卡了”，S愤愤的骂着，到各个群里喊话“有没有能对接A平台的（卡商）?”。实在没有他就得走接码平台的项目，每个号要多两毛钱成本。

除了卖账号，S专门分了一个人手，每天专门采集、修改视频。群控自动上传作品，当作品出了播放量就留下微信号，进行引流，每天能出八九千的粉，每个一块一。



群控用了一段时间，非常顺手，S便给自己的徒弟出了一套群控。听说盗号的L被抓了，也是，L都做了两年了，每天出几千个，结果被下游撸包（在微信中发有色视频，欺骗性的索要红包等行为）的连带了。L的事情在圈子里讨论激烈，S后来新收的十几个徒弟都是在广东面交了的。

S开始出售群控系统，做A平台三种账号的全部脚本加工具，卖两千，加上引流自动上传作品、修改用户资料等一系列功能，再加一千五。可好景不长，才两三周，群控

出了没几套，他的号开始死了，只有五成存活，每次要给客户补号，很是麻烦。

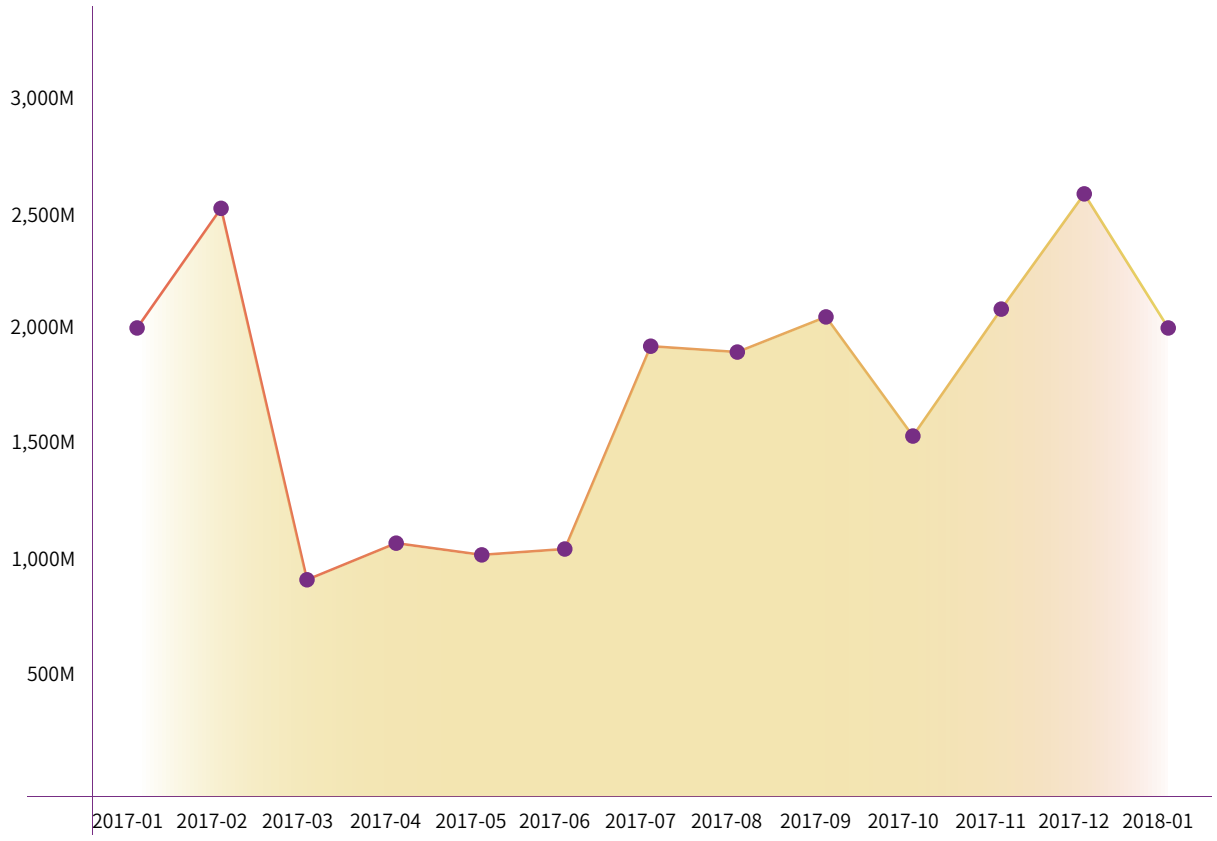
“不知道平台是怎么判断的，技术正测着呢。”，S猜测会对设备信息进行检测，他做号和用户使用的时候设备信息是不同的。S便在平台上出售带设备信息的账号，可是这种设备信息需要特定的工具，会用的人少，很多人扔掉了A平台，去别的平台做了。

“就是一短信激活，这有的号就死了。现在主要卖粉了，没原来好，但还可以。”S每天只能卖出两三千号，没有大客户了。主要项目就成了出粉，S说每消耗两三百个账号，可以出三千左右的的粉。也可以手动操作没激活的号，能保证八成的号不死，可人工做一天都很烦躁。

S说自己想先稳住A平台，同时在测试一些新兴的小平台，出引流脚本挣钱。现在手里有一个项目很好，目前是手动操作，要解决的问题是，平台不允许越狱手机登录，就不能上脚本自动跑。“我感觉A平台以后有赚，得坚持下去，我手里的陌陌账号，两年前就在用，现在还可以出粉。A平台才几年呀?那些小平台很容易，但是不知道什么时候会死。”

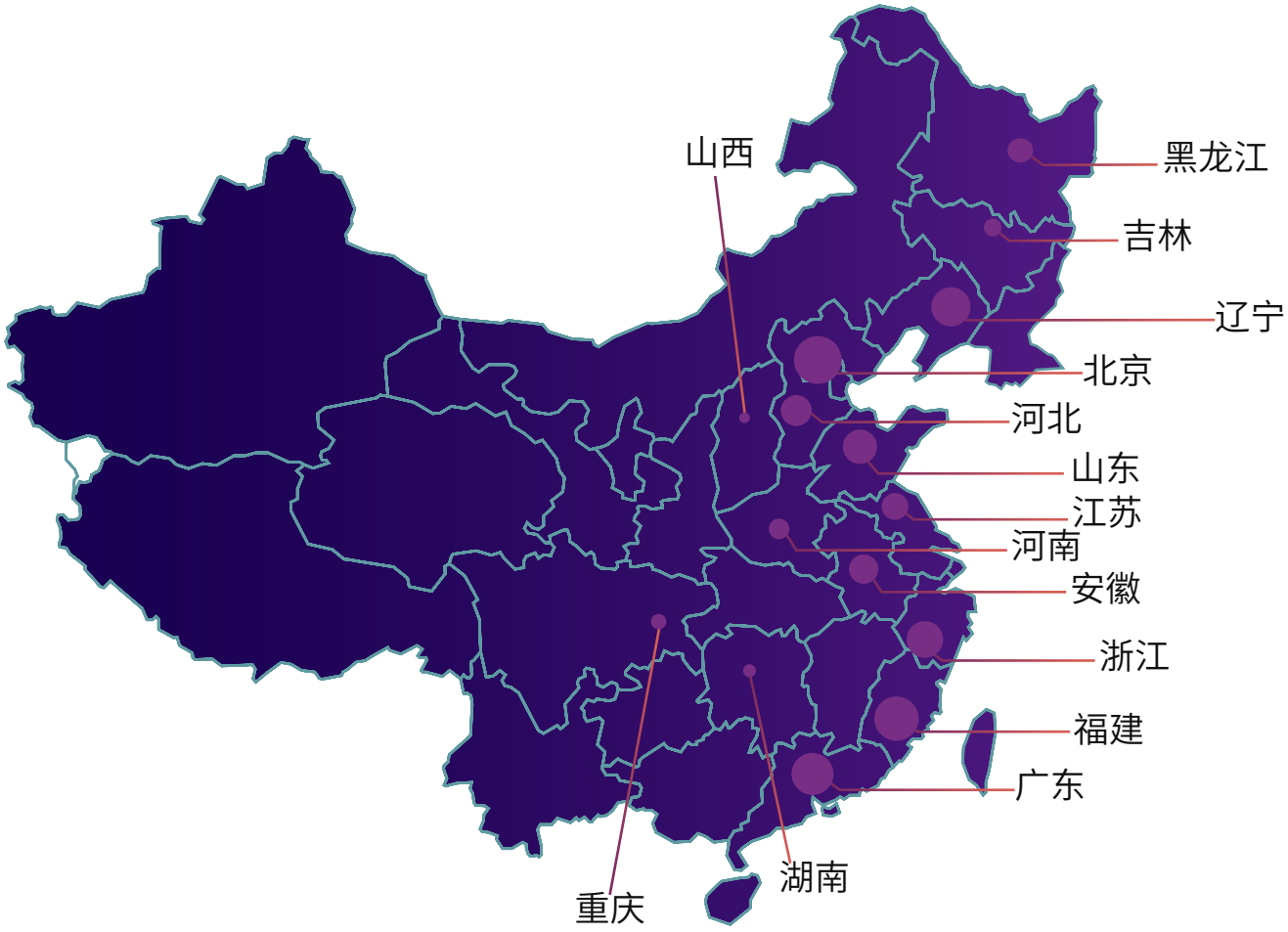
4.1.3 数据分析

根据威胁猎人捕捉到的短视频平台风险数据，经过分析可以得出2017年短视频平台遭受攻击的趋势变化，以及团伙的地域分布。其中，2017年年初（2月）及年末（11月、12月）的攻击量处于峰值，与各大平台年初与年底的营销宣传活动有关。在2017年短视频平台全年攻击分布中，数值最低的一个月数量也达到了10亿左右，月平均攻击量月20亿次，攻击团伙的疯狂程度可见一斑。



短视频平台全年攻击量变化

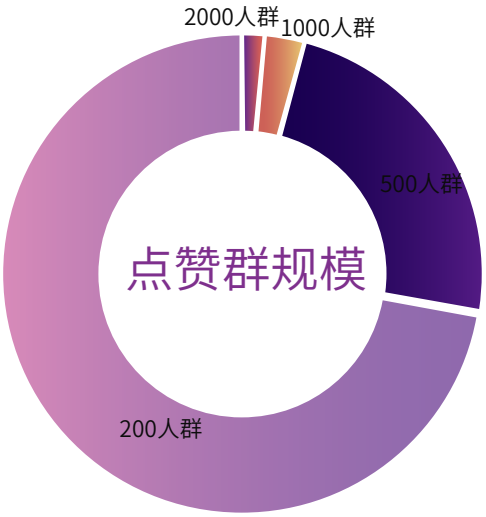
攻击团伙的IP分布情况显示，最大的攻击IP来源地是北京，紧随其后的是福建省和广东省。全部攻击IP遍布全国15个省、市或地区。



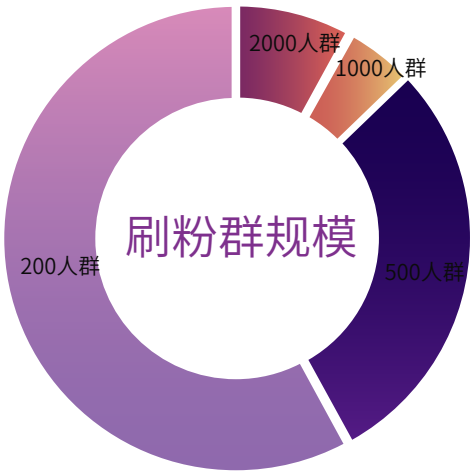
短视频攻击团伙IP分布

此外，以“点赞”、“刷粉”、“引流”等词语为关键词，结合排名较靠前的短视频平台对QQ群进行抓取，发现相关的QQ群数量庞大，地域分布也呈现一定的特点。

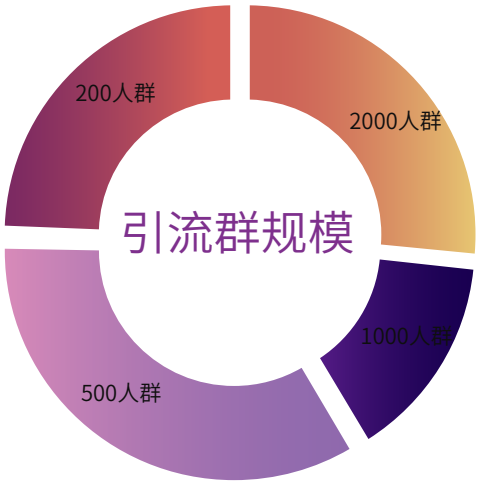
通过统计相关QQ群的平均人数，发现引流QQ群平均人数最多，达到601.99，刷粉QQ群平均拥有299.64个群成员，而点赞QQ群则平均拥有83.13个群成员。



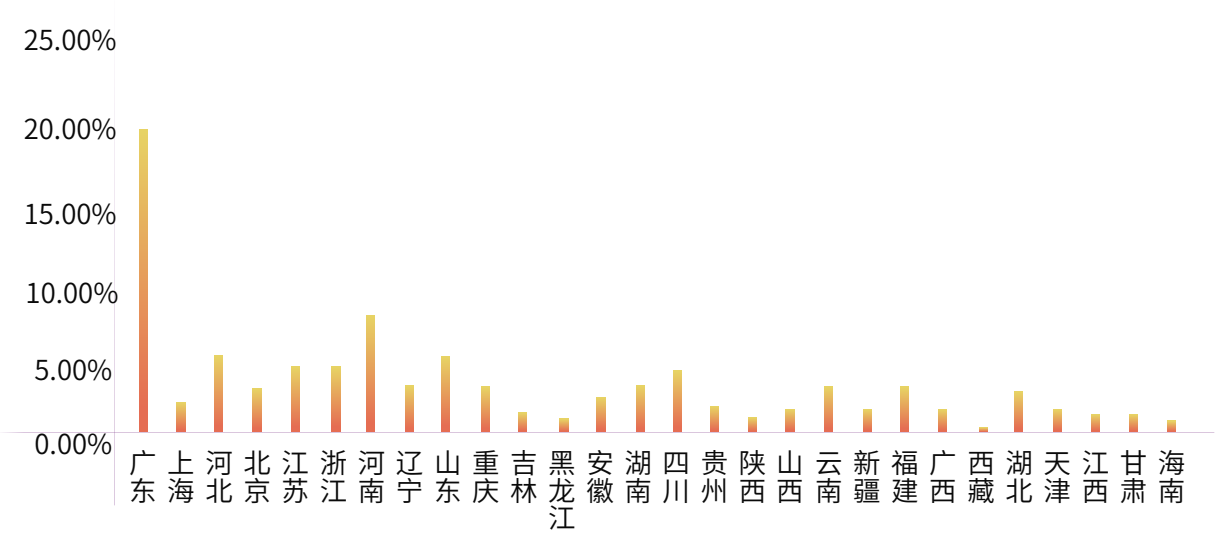
点赞群的群规模分布中，200人群为主流，占到72.27%。在刷粉群中，也有类似的分布情况：



在引流群中，占比最大的是500人群，达到34.11%，2000人群占到26.53%，200人群则占24.49%。

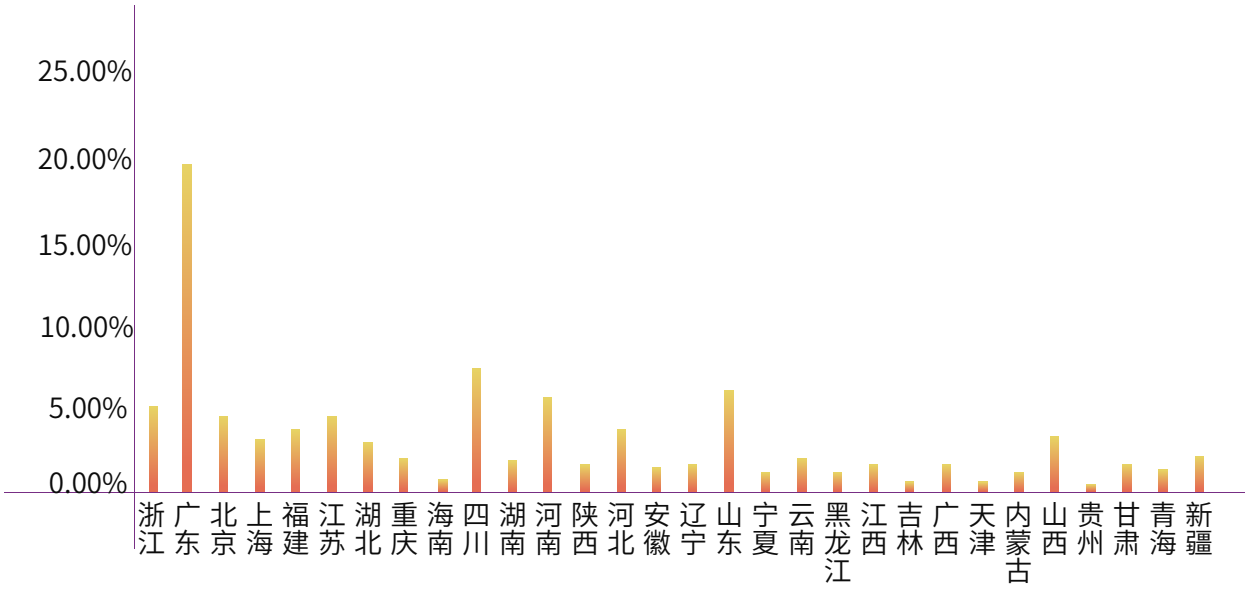


与答题应用相关群不同的是，搜索结果中没有找到规模5000人的群组。



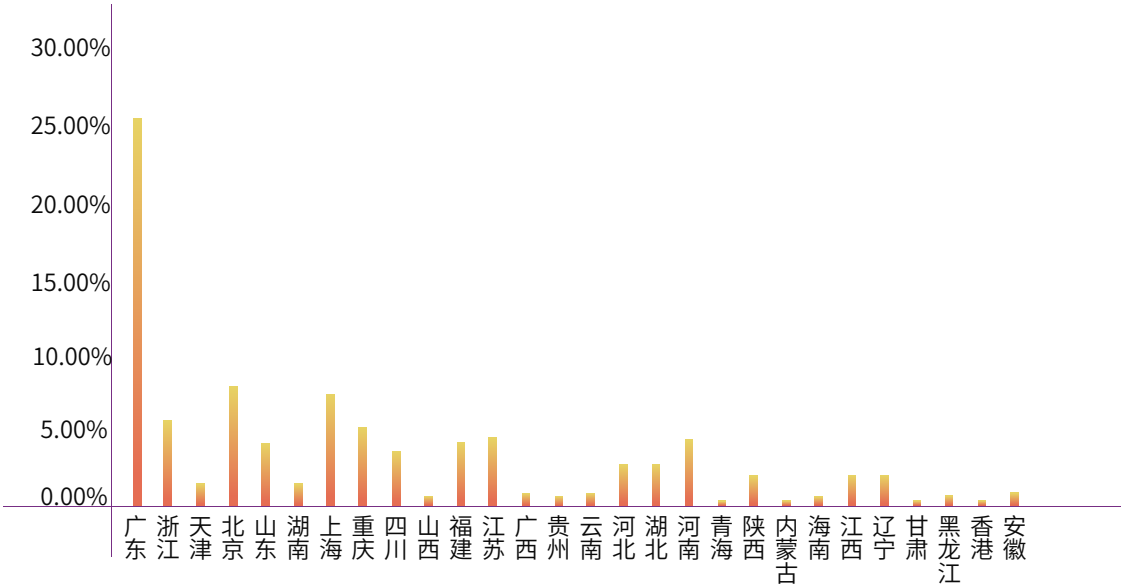
点赞QQ群地域分布

从地域分布来看，点赞QQ群在广东分布最多，占比达到20.12%；其次是河南，占8.98%；山东位列第三，占比6.19%。



粉刷QQ群

在刷粉QQ群的地域统计中，广东省位列第一，达到20.27%；四川省位列第二，达到7.64%；山东位列第三，达到6.31%。



引流QQ群分布

引流群显示了不同的规律：群地点位于广东的QQ群，占26%；其次是北京，达到8.67%；上海位于第三，达到8.33%。

通过以上分析可以看出三个环节的成熟情况：引流产业规模最大，而这三种产业环节都在广东发展较成熟。在群地域分布规律中，广东、山东、河南位列前列，而这三个省都是人口大省，反映出这些产业与人口分布的关系。

4.2 直播答题黑灰产团伙

4.2.1 行为分析

根据各个平台直播答题的规则，全部答对12道题确实不太容易，所以平台允许一次复活机会。按照规则复活机会除了官方活动之外只能通过邀请新用户加入并填写邀请码来获得，因此刷复活码也逐渐形成了链式推广。此外，卖题库、卖答题外挂也成了黑灰产的盈利手段。

一般平台对于复活机会不设上限，也就是说，能邀请多少新号填写自己邀请码就能获得多少次复活机会。为此，淘宝上很快出现售卖复活卡的链接，单价一元或者0.5元，看起来非常便宜，这其实跟刷粉丝数差不多，通过某种方式创建无限小号，成本也是非常低的。

除了购买复活卡来提升瓜分奖金的机率之外，确保答对全部题目显然更加靠谱。因此部分人总结出所谓的出题规则，比如常识、历史上的今天等，在淘宝或者QQ群公开售卖题库。不过，题库蒙题的成功率并不理想。在国内以QQ和微信为主要线上交流渠道的当下环境中，拉群集思广益一起答题成了答题玩家以及黑灰产的首选。在QQ群搜索各个答题平台的关键词，可以搜到大量相关的群组，有些群进群还要付费。

不过，受到热捧的还是答题辅助软件。一般在直播答题中，问题会以文字形式出现在屏幕上，同时主持人还会语音念出题目。这也让一众软件开发者急中生智，利用语音识别或者OCR识别的方式在问题出现后，迅速调用搜索引擎搜索问题以及答案，10秒钟的答题时间手动百度几乎不现实，而通过软件完全可以找到正确答案再选择。目前，这种软件在淘宝、各种QQ、微信交流群广泛传播，种类也非常多，自己开发或者盗用别人开发的软件公开售卖的现象，比比皆是。

4.2.2 直播答题黑灰产发展时间轴

2018.01.05

出现大量付费Q群。每到答题时间，群主或管理员就会开启禁言模式，用1，2，3位代号代表答案；或者多名群成员进入群语音分享答案（并不保证正确率）。有些群只是简单维持秩序，群内成员可以分享答案。群里也会销售一些复活卡。

在这些群里，“吃鸡”有了另一层含义。一般答完一场题目并成功分到奖金，就叫“吃到鸡了”。

“吃鸡”截图

但是此时，针对直播答题的盈利模式还没有形成，即这些群主的目的不是盈利。只是用付费的方式筛选出愿意花钱的一些用户，当之后直播答题出现可以批量操作的“玩法”时，这些人就是会付钱的优质流量，即使直播平台最后没有合适的“玩法”，这些人同样可以用在以后的项目里。

这时候刷复活卡的方式是使用模拟器手动批量操作，羊毛党也在试验测试中。

2018.01.08

开始有人发出“西瓜视频注册邀请机”的工具定制需求。

2018.01.11

出现使用Fiddler刷复活卡的方法，12日晚该方法失效。卡商开始活跃，发出“直播答题”的专属对接码，侧面说明此时已经有很多人需要大量的手机号，供给注册机去批量注册、填写邀请码了，即他们手中已经有了批量注册的工具。

定制软件后，操作人会对接一些卡商，进行注册。当卡商们大量开始宣传，发出对接码的时候，说明已经有了成熟的注册方式，且对黑卡手机号需求较大。

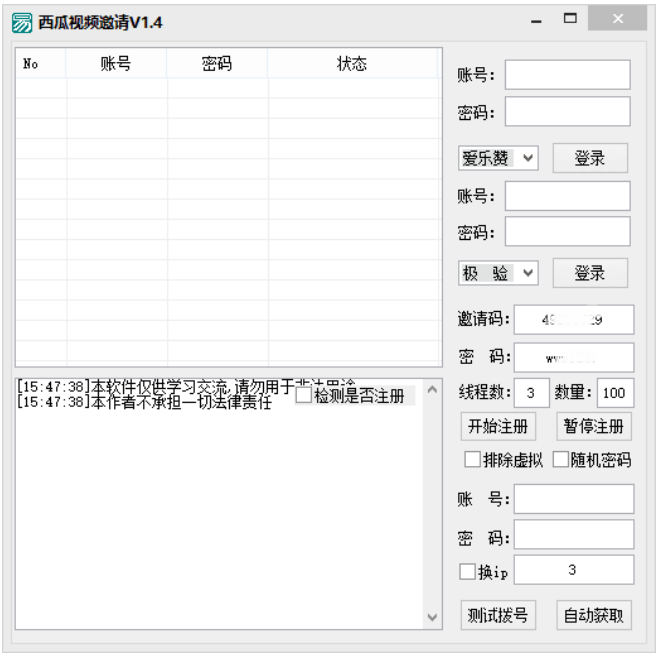
2018.01.12

出现各类薅羊毛教程，这些教程根据各平台特色、提现方式、提现起付额度等做了详尽的分析。平台逐渐出现了对抗的策略，如对单个设备注册数量进行限制等。手动注册的人采取每次都新开模拟器的方式（每次新开，是一套新的设备信息），绕过平台的设备检测，实现批量注册。

2018.01.14

销售复活卡的人数增多，兜售百万英雄的注册邀请机等的行为也开始出现（注册机使用人数大幅增加的前兆）。

各大平台的注册机原理大都相同，工具开发人将模板做出简单修改就可以，平台开始对IP做出限制使，开发者就加入“代理IP平台”的模块，整个修改过程不需要很长时间。



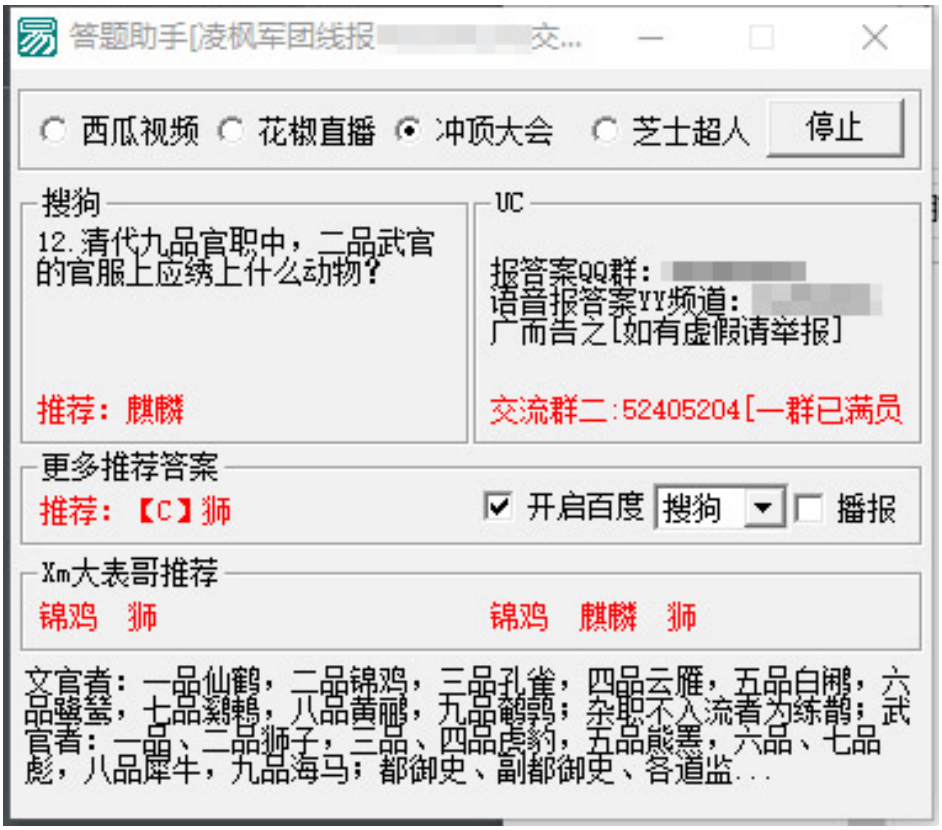
1、软件支持西瓜、花椒、芝士、冲顶四个平台单IP无限草复活卡

2、软件需要接码，已对接（爱乐赞，玉米，短租，神话）

3、西瓜和花椒带老号检测，芝士和冲顶没有老号检测接口，所以一定要找卡商新号对接比较稳

2018.01.15

出现各类答题助手和各个平台注册机工具。出现大规模薅羊毛行动，薅羊毛形成模式，方法逐步分享在各个薅羊毛线报群中。如下图答题辅助工具集合了各个平台，实际测试，此工具2-3秒后就可以显示答案，工具也接入了人工的模块，降低了AI搜索错误造成选择错误的风险，给羊毛党提供了便利。



2018.01.16

复活卡价格降低至0.6-0.8元，使用微博授权号的人增多，微博授权号普遍几分钱一个，相比使用手机号注册，成本降低了一半。于是有人开始出微博授权号的注册机。

主要收uc！西瓜！ 其他app项目价钱略低。
要求：1.多线程
2.必须能对接网站api，我网站有人下单，软件就自动获取订单然后自动开单
3.支持手动增加订单
4.需要导入微博小号的话，顺便加上导入cookie
5.能拨号换ip，可以设置注册到第几个号后换IP
6.接码支持短租，爱乐赞。如果需要打码支持若快，超人
7.我这有4台电脑，软件可以绑机，都得帮我注册
8.软件包一周售后

2018.01.18

复活卡价格降低至0.5-0.7元，答题辅助软件开始泛滥，百万英雄推出了组队玩法，“玩家”开始尝试组队。

2018.01.19

邀请码传输过程中经过加密，一些作者分享了相关算法，方便使用工具批量进行操作。

算法分析

复制代码 纯文本模式

```
' 0x0A 固定标志头
' 0x08 邀请码长度
' 0x38, 0x37, 0x39, 0x38, 0x32, 0x35, 0x32, 0x33 邀请码字节集
' 0x10 固定的
' 0x20 'aid=32 appid 的十六进制 现在是固定的
' 0x18 固定的
' 0x80, 0xF6, 0xE4, 0x8B 经过加密device_id 加密算法 EnCrypt_Did 已经改好了
' 0xAF 经过测试，这个是属于添加字符，直接随机2个字母即可
' 0x01 固定的标志尾
```

EnCrypt_Did 的算法也打包了，大家自行下载，如果觉得不错，请给予好评

模块用精易模块就可以了

西瓜视频填写邀请码算法.zip (216.5 KB, 下载次数: 265)

之前的帖子
西瓜视频_EncryptWithXor纯算法源码

2018.01.20

答题辅助软件和注册机都在不断更新，复活卡价格降低至0.4元。

2018.01.23

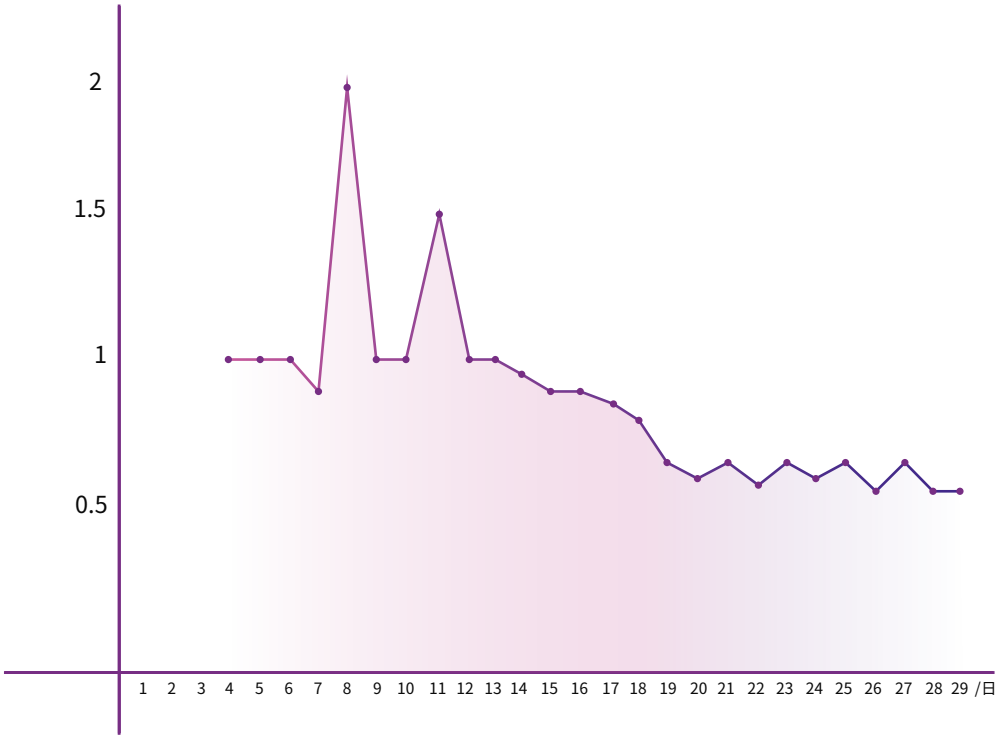
复活卡价格降低至0.35–0.38元。

2018.01.25

部分作者开始分享源码，侧面证明了工具使用的泛滥，工具非常容易拿到，源码的价值也没有那么高了。注册邀请机根据平台限制不断在完善。

2018.01.26

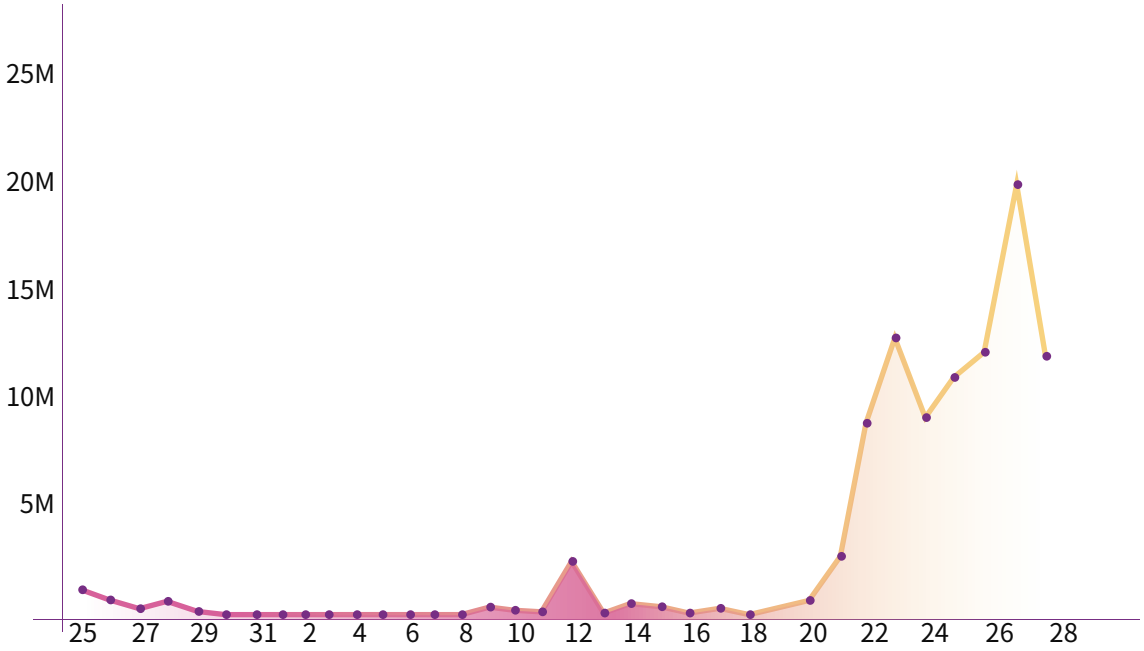
复活卡价格维持在0.3-0.4元。



2018年1月份直播答题复活卡价格变化图

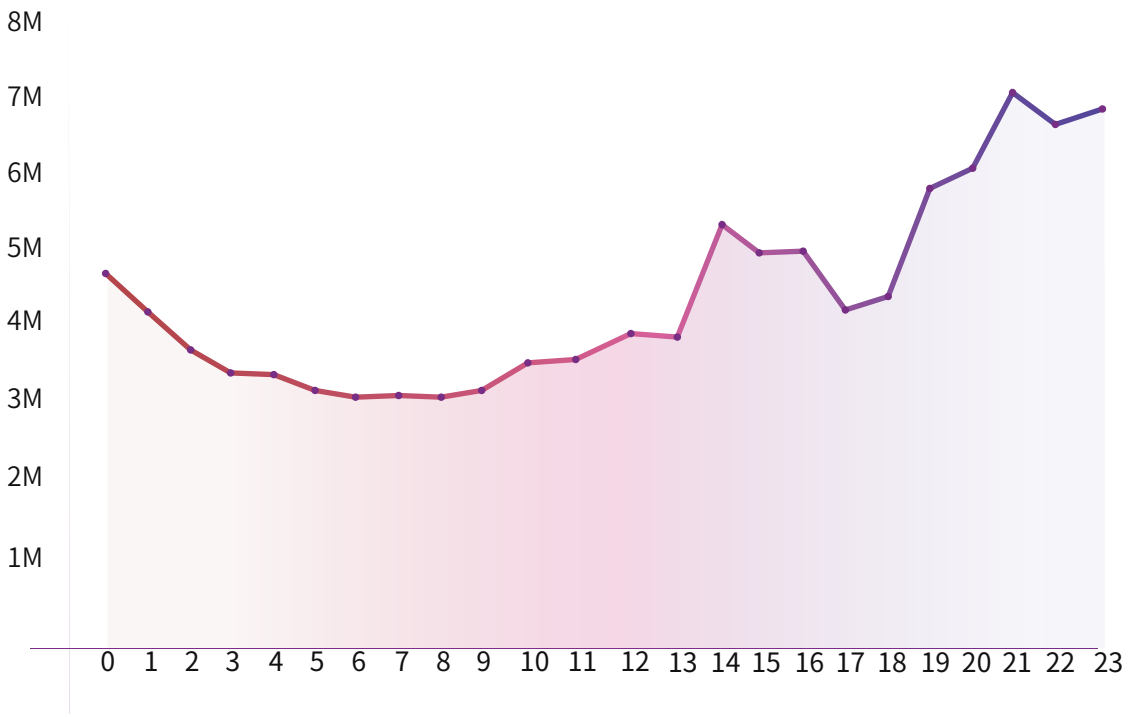
4.2.3 数据分析

根据威胁猎人捕捉到的直播答题平台风险数据，分析可得出直播答题爆火的这一个月以来的攻击趋势变化。直播答题出现的前20天左右，攻击量平均在50万以下，此时面对新兴的平台和模式，团伙还在探索之中。1月20日之后直播答题平台遭遇的攻击量激增，到1月27日达到顶峰，超过2千万。



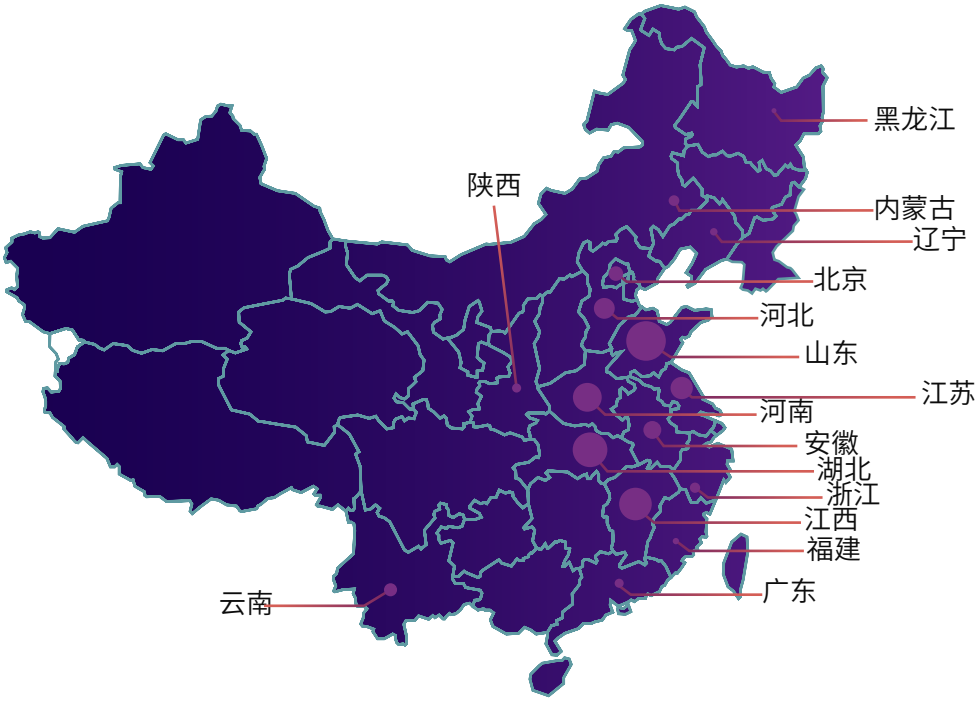
直播答题近 1 个月攻击量变化

此外，24小时内的攻击变化也体现了一定的规律。除了黑产团伙惯用的深夜作案这一特点，一天内直播答题平台遭遇的攻击次数与其每天答题开始的时间有关，每到答题时间，攻击量就会上涨。

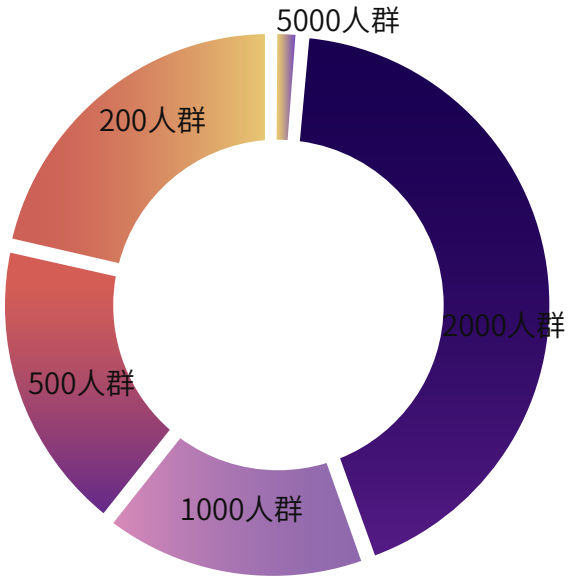


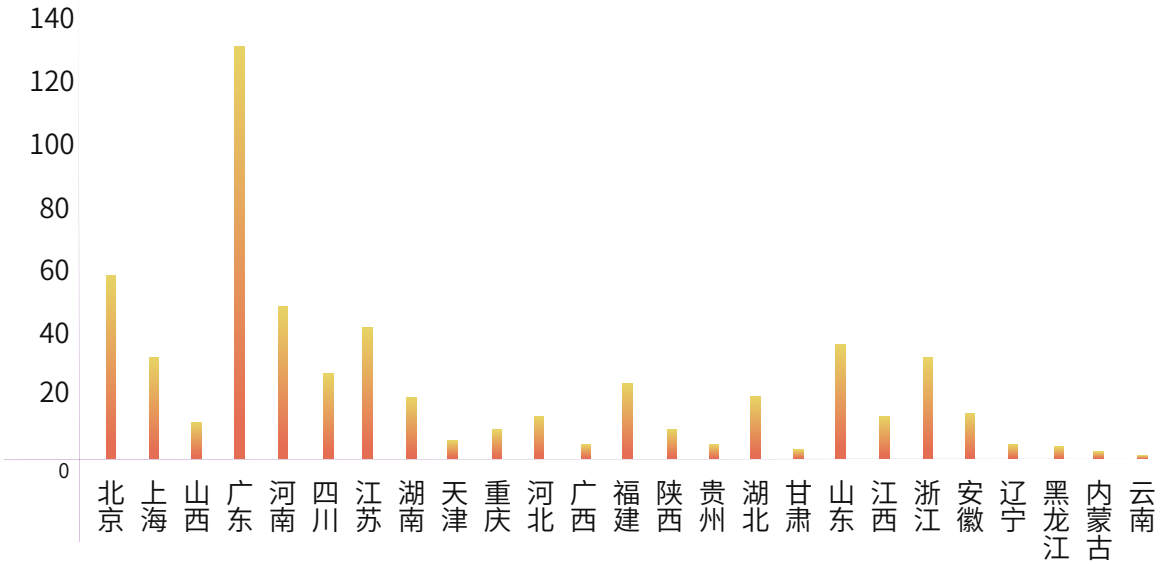
24 小时直播答题攻击量变化

攻击团伙的IP分布情况显示，最大的攻击IP来源地是山东省，紧随其后的是湖北省和江西省。全部攻击IP遍布全国16个省、市或地区。



此外，通过对QQ群关键词的抓取发现，直播答题相关的QQ群数量庞大，总数将近700个。近半数QQ群组的规模达到2000人，占比43.13%；1000人群占总数的16.08%；500人群占比17.84%；5000人群和200人群分别占到1.46%和21.49%。这表明，通过QQ群交流答题答案已经成为了一种较为广泛的现象。





QQ群地域分布

在所有群组所设定的群地点中，广东省的占比最大，达到22.35%；北京市位列第二，占到9.92%；河南位列第三，达到8.24%。广东、北京、河南、江苏、山东位于前五，一定程度上说明，这些QQ群的分布与地区发达程度、互联网基础设施相关程度不高，与实际人口分布相关。

第五章 应对方法与安全建议

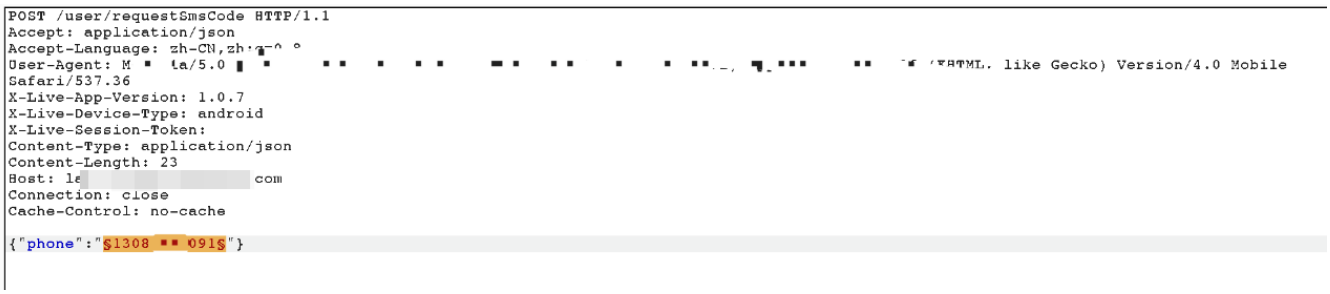
以“冲顶大会”为代表的直播竞答和以“快手”为代表的短视频平台最大的隐患，在于机器流量、广告引流、垃圾信息、薅羊毛等几大问题。要想应对这些问题，需要从上游环节或者技术上进行控制。此外，合规与监管方面也需要注意。

5.1 企业应对流程

5.1.1 案例

由于问答型app最近火热，上线比较快，并没有考虑过多安全方面问题。于是就会出现一些常规的安全问题，比如短信接口控制不严，可以滥用短信接口，导致短信轰炸影响用户以及消耗厂商信息资费。

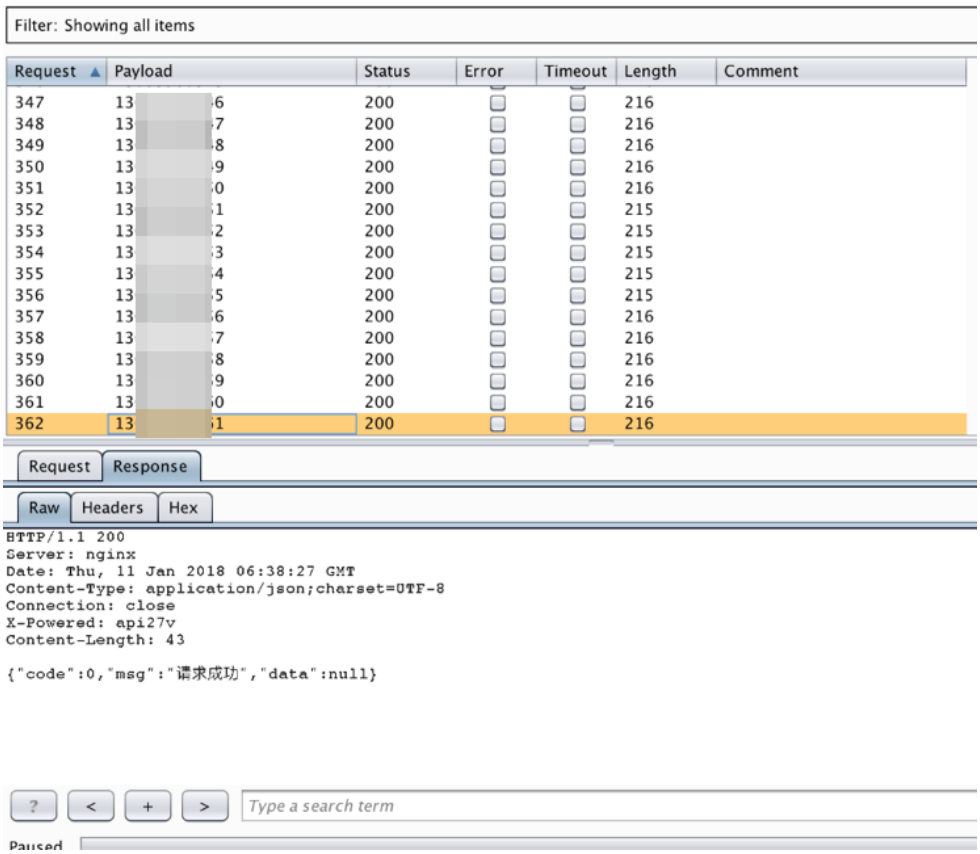
输入手机号发送验证码，截获发送验证码请求包。



```
POST /user/requestSmsCode HTTP/1.1
Accept: application/json
Accept-Language: zh-CN,zh;q=0.8
User-Agent: Mozilla/5.0 (Linux; U; Android 4.4.4; zh-cn; MI 4LTE Build/KTU84P) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Mobile
Safari/537.36
X-Live-App-Version: 1.0.7
X-Live-Device-Type: android
X-Live-Session-Token:
Content-Type: application/json
Content-Length: 23
Host: le[redacted]com
Connection: close
Cache-Control: no-cache

{"phone":"$1308[redacted]091$"}
```

遍历手机号，可对无限量的手机号发送短信验证码请求，返回成功。



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
347	13[redacted]6	200			216	
348	13[redacted]7	200			216	
349	13[redacted]8	200			216	
350	13[redacted]9	200			216	
351	13[redacted]0	200			216	
352	13[redacted]1	200			215	
353	13[redacted]2	200			215	
354	13[redacted]3	200			215	
355	13[redacted]4	200			215	
356	13[redacted]5	200			215	
357	13[redacted]6	200			216	
358	13[redacted]7	200			216	
359	13[redacted]8	200			216	
360	13[redacted]9	200			216	
361	13[redacted]0	200			216	
362	13[redacted]1	200			216	

Request | Response

Raw | Headers | Hex

```
HTTP/1.1 200
Server: nginx
Date: Thu, 11 Jan 2018 06:38:27 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
X-Powered: api27v
Content-Length: 43

{"code":0,"msg":"请求成功","data":null}
```

? < + > Type a search term

Paused

针对这个案例，可以限制短信接口的访问频率以及速度；同时加入图形验证码，避免机器发包，进而避免相关的安全问题。

5.1.2 应对方案

事实上，短视频平台与黑产之间的博弈战一直在进行。例如，今日头条专门针对刷粉行为，根据粉丝活跃程度、信息完整性、异常涨粉等行为进行“非真实用户”评估。同时，各大短视频平台也逐渐提升审核机制，几乎每周、每个月，都会公布一系列涉及垃圾营销号或者标题党帐号的封禁公告。

但是，在短视频行业的黑灰产中，下游的具体黑色行为与账号、卡号、工具等密切相关，要相应对这些问题，还是需要从上游环节入手，进行对抗。

针对手机黑卡、代理IP

卡商、代理IP、工具开发等产业，不只是针对短视频平台，分别深挖都是一条完整的产业链。对于这一环节，作为企业，最快捷的方式是从专业公司获取经过审计的手机黑卡、恶意IP、高危账号等数据。将其作为自己后台黑白名单数据的补充情报库，在注册或活动流程中接入审计策略，对恶意注册进行筛选监控等。

更新及时、有效性高、数据全面的情报库，可以让企业投入的经费能得到有效利用，尽量减少因黑卡等产业带来的损失。

针对账号商人

除此之外，各平台可以对账号商人进行打击。账号是各个后续产业的必备资源，当账号资源变少，后续的产业都会受到影响。结合短视频平台的特点，威胁猎人给出如下建议。

结合恶意数据情报库，对可疑用户提高注册门槛、增加复杂验证码等，并对这些用户进行重点监控，当其进行敏感操作时，进行防护。恶意数据情报库包括：黑产掌握的黑卡号码、使用的代理IP、已经泄露的账号密码数据等。一方面要结合自身后台数据的黑白名单，另一方面也要引入第三方的支持，进行更全面的检测。

针对黑产技术人员

黑产工具开发人员会针对平台的注册流程，进行攻破，如接入打码平台填写图形验证码等，以实现批量化操作，对于这类问题。企业需要擅用黑产产业链情报。如分析黑产的注册流程和攻击工具。批量行为都是有迹可循的。企业可以针对恶意用户的行为偏好和其在黑产中的使用广度，在设备信息、注册信息重合度、恶意用户的行为数据等方面，进行多维度的判断。根据其攻击目的，在适宜的地方增加对方的攻击成本。

如，针对疑似羊毛党用户，在提现、积分兑换礼品等地方，提升操作门槛，要求验证绑定的手机号等。结合产业链情报，企业就可以针对攻击场景和攻击目的，进行更精准的打击。

从另一个层面来说，平台在自身运营时，也要注意从事前准备、事中监控&响应、事后总结这三个环节入手，来确保业务安全。产品或业务上线前，可以借助第三方安全厂商或白帽众测服务查找漏洞并修复；在涉及与开发阶段就考虑到风控等需求，适当引入第三方风控服务。在运营过程中，可以依赖大数据、IP与账号黑名单等，在关键阶段进行门槛性限制。同时准备好应急预案，在运营过程中持续监控，一旦发现问题，就及时响应。风险事件发生后，

除了迅速应对，还要对异常行为、异常账户、异常数据等进行分析，抽取相关的IP、账号等信息，沉淀为历史数据，供以后使用。必要时，可以报警调查，并根名单数据，追回风险事件所造成的损失。

以当下大火的“冲顶大会”为例，通过风险设备识别、行为风险识别、关联风险识别等策略模型针对机器作弊行为进行防范，可以有效鉴别机器流量，解决直播答题场景中的“机器注册”、“机器登录”、“机器流量”等问题，从源头识别欺诈风险。

此外，采用OCR识别和NLP技术，可全面高效识别文字、图片内的垃圾广告，仅微信变体就已识别数千种，可有效清除导流广告、变体广告等。

5.2 加强合规监管

2017年6月1日,《网络安全法》正式实施。《网络安全法》的出台具有里程碑式的意义,此次立法进程的迅速推进,显示了党和国家对网络安全问题的高度重视,是我国网络安全法治建设的一个重大战略契机。

《网络安全法》第二十二条规定[6]:

任何个人和组织不得从事入侵他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动;不得提供从事入侵网络、干扰网络正常功能、窃取网络数据等危害网络安全活动的工具和制作方法;不得为他人实施危害网络安全的活动提供技术支持、广告推广、支付结算等帮助。

短视频行业黑灰产的肆掠,显然已经影响到平台的利益,影响到普通网民的上网行为。不法分子利用网站漏洞非法牟利,已经触犯法律。号商、微商和各级代理间也同时存在盗窃、诈骗等犯罪行为,监管部门应当加大执法力度,杜绝此类利用“风口”项目进行黑灰产业的非法行为。尤其是黑卡、黑IP等黑灰产大行业的上游环节,更应当严肃应对,严厉打击。

事件发生后,监管部门应尽最大的可能的保护受害者权益,尽可能多的追回损失。这对于受害者的保护、对于市场环境的监管、对于监管部门形象的塑造、对于社会风气的引导,都有积极作用。

5.3 提升安全意识

2017年《中国网民网络安全意识调研报告》[7]调查显示，约九成网民认为当前的网络环境是安全的。其中，49.1%的网民认为当前的网络环境比较安全；32.8%的网民认为一般安全；6.9%的网民认为非常安全。

网络安全防范能力方面，网民更是体现了充分的自信，43.7%的网民给自己打了4分，14.4%的网民给自己打了5分。

然而，网络安全意识的提升绝不只是一两次调查和一两句口号就能做好的，必须脚踏实地的组织安全培训、加强安全管理、学习安全知识，从根本上提升公民的整体安全素质，才能真正使不法分子的违法行为成为无源之水。

5.4 小结

流量利用与变现，是黑灰产亘古不变的追求。本报告从短视频出发，也只是窥探到了流量利用的冰山一角。黑灰产的触手，已经延伸到互联网的每个角落。每个人，都身在局中，都要尽力探求真相，更要保持清醒。

附录

参考来源

[1]《2017年中国移动互联网年度报告》, QuestMobile
https://www.questmobile.com.cn/blog/blog_127.html

[2] 第41次中国互联网络发展状况统计报告》, CNNIC
http://cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/201801/P020180131509544165973.pdf

[3]《风口来袭, 谁主沉浮?——36Kr短视频行业研究报告》, 36Kr
http://research.36kr.com/generic/web/viewer.html?id=88

[4]《2017 中国短视频行业研究报告》, 艾瑞咨询
http://www.iresearch.com.cn/report/2643.html

[5] 百度搜索指数 http://index.baidu.com

[6]《中华人民共和国网络安全法》, 全国人民代表大会常务委员会
http://www.miit.gov.cn/n1146295/n1146557/n1146614/c5345009/content.html

[7]《中国网民网络安全意识调研报告》, 360 安全卫士
http://www.freebuf.com/articles/paper/151673.html

关于报告

作者

FreeBuf 研究院：鲍弘捷、曾裕智、朱嘉豪、施东奇、朱伊琳、余桂茗

威胁猎人：朱科锭、陈南利、梁倍毓、张晓杰、薛欣原

美术设计：姚媛媛

深渊背后的真相之「短视频黑灰产业」报告

威胁猎人 THREAT HUNTER

FREEBUF