引流黑产调查：

一个“色粉”2元 炒股粉60元

当陌生“美女”或“帅哥”向你发来打招呼的信息时，有人会深信不疑索要联系方式，有人则会怀疑对方是不是骗子。实际上，在多数情况下，对方既不是帅哥，也不是美女，而是机器程序。

2019年12月20日至26日，记者对黑灰产“引流”产业链进行调查发现，黑灰产已经逐渐分出了引流与变现两个分工明确的上下游产业：上游通过话术、广告点击或者流量劫持获得“粉丝”并引流至下游，下游再通过推销“黑五类”产品或诈骗进行变现。在这一过程中，每个在上游“上钩”的用户都会被打上“××粉”的标签，被明码标价卖给下游商家，而群控软件、引流脚本等外挂设备则是上下游黑产共同需要的“辅助工具”。

“引流产业其实就是营销黑产，其特点是大量利用正常公民的身份信息，绕过平台限制规则，发送大量涉黄涉政、低俗广告等引流内容，并最终以诈骗等形式变现。”反欺诈实验室专家李柚（化名）说。

李柚对记者表示，引流诈骗需要大量他人身份信息，这会导致公民信息买卖黑产的肆虐；而根据行业不同引流的粉丝价格也不同，其中交友网站上男性粉丝引流难度较低，价格也较便宜，这意味着有更大的流量被用于诈骗；此外，网络账号对于引流产业来说是消耗品，这使得互联网平台的管理难度成本增加，资源消耗增长。

加陌生人好友被当“色粉”转卖

“宝宝一个人在家好无聊，可以加我微聊天嘛，我的微信……”。2019年12月19日，某交友平台用户小袁收到了一个名为“雪儿妹妹”的用户息。小袁试图和“雪儿妹妹”聊天，却发现对方除了加微信这一句话外一言不发。小袁添加了微信后发现，其微信头像以及用户名完全不是之前的“雪儿妹妹”，没说几句话，对方就以手机没话费了为由要求小袁打钱。

接近灰黑产的人士Adan告诉记者，实际上，小袁在交友平台上与微信上所接触到的“雪儿妹妹”分别来自两个黑产团队，“前面一个负责引流，后面一个负责骗”。

记者近日接触了数家提供“引流出粉”服务的黑灰产团伙发现，光“引流”一项服务，现在市场上就已经发展出了至少三种不同的花样，而提供引流服务的商家则多以“工作室”或“营销公司”的身份活动。

一家营销公司工作人员介绍，提供通过“群推广与APP话术引流”的各类男性粉丝，“全国单价3元一个，地区粉3.6元一个”。而对于赌博粉丝、炒股粉丝等价值较高的人群，则主要通过网页广告与流量劫持模式进行吸粉操作，“网页广告需要首充6000元，粉丝量要看你的广告效果，流量劫持60元一个粉丝。”

根据反欺诈实验室提供的资料，被上游的引流团伙导入到下游的流量会被分为色情流量、股民流量、车主流量、赌徒流量、兼职流量、租房流量等多个类型，再以不同的价格卖给定向诈骗团伙或黑五类产品销售人员，进行变现。

Adan向记者透露，现今能够作为引流的平台很多，“只要能发送私信、评论，任何平台都能成为引流的场所，比如现在微博评论中泛滥的‘卖片哥’，你加他好友的一瞬间，可能自己就会被打上‘色粉’的标签，被一个黑产团队卖到了另一个黑产团队。”

记者观察发现，在各类粉丝中，引流需求最多、量最大，价格也最便宜的当属“色粉”，而对此类粉丝最便捷的引流方式就是话术引流。2019年12月22日，记者为调查找到一家提供“各个平台色粉引流”的黑产工作室。该工作室负责“市场营销”的人士小赵表示，微信色粉的引流成本为2元一个，主要引流方式就是话术引流，要求提供简单易懂的微信号或关联QQ、手机号，并采用扫码登录的方式登录对方PC端，“到时候粉丝会自己来加你的微信，你只需要通过好友申请就行”。

记者于当日14点向对方提出了相关要求，截至当日21点，记者的微信上果然新增了100个好友申请。而接受申请后与这些“引流”而至的粉丝聊天发现，这100人之所以添加记者微信，是因为在探探、×聊、××漂流瓶等不同的交友APP上收到了含有记者微信号的引流信息。

一家主做网页广告吸粉的工作室人员则表示，根据粉丝类型的不同，吸粉的成本也不一样，“最好引流的是漫画、小说行业粉丝，这些一般都只用‘色粉’就行，成本在6到8元，而最难吸粉的是网赚、餐饮加盟等粉丝，成本要高达100元一个。而情感咨询、减肥等行业的粉丝则处在中游，基本上60到80元一个。”

让你加好友的诱惑美女是“引流”机器人

“实际上，这些工作室都是事先编辑好引流的话术文案，再使用脚本发送至不同的平台上，通过私信或评论触达潜在的‘粉丝’，达到自动发送引流信息的目的。”Adan告诉记者，“你看到的让你加她好友的私信，其实都是机器人自动发送的，根本不是什么美女。”

李柚表示，引流团伙会想尽办法绕过平台限制规则，因为不管什么样的APP都不会允许用户大量利用自己的平台发广告信息，但引流团伙目的是曝光，它会利用任何地方曝光，包括头像签名等，引流团伙也会想方设法地绕过包括破解监控里面的通信协议、算法，最后达到批量发送的目的。

记者发现，除了小赵所在的分工明确的微信团队，目前市面上也有“自助型”的引流脚本贩卖。今年5月，记者曾在二手交易平台上搜索到涉及抖音、全民K歌、珍爱网、Soul等各个平台的多种类引流脚本，价格从1元（单个平台）到388元（多平台打包价）不等。

记者以35.2元的价格在一个商家手中购得一套包含喜马拉雅、微信、抖音、美拍、探探等22个平台在内的“定制版引流脚本”。

打开该脚本后，记者发现其“功能设置”中包括视频评论、粉丝私信、粉丝关注、评论私信、评论关注、评论点赞、好友私信共7项功能，在该页面，用户可以手动输入评论话术与私信话术，此外，还可以进行发图设置、重复发送、添加关注、双话术等常规设置，亦可筛选男女。

脚本不仅可以用在引流这一“上游”中，引流后的诈骗话术照样可以用脚本完成。在Adan提供的一套“护士借钱”诈骗话术中，黑产从业者将微信号包装成从异地来中医院上班的实习女护士，在5小时的时间内平均每20分钟向“粉丝”发送一条信息，整个话术从熟悉、亲近到以“给妈妈订车票”为由借钱，再到最后拉黑，一气呵成，均由机器脚本完成，虽然成功行骗的概率不高，但利用脚本以及多开工具，行骗成本极低，可以“广撒网”进行诈骗。

记者注意到，不少从事引流吸粉黑产的团队往往也代卖软件和技术，甚至提供“贴牌”服务，如“JK爆粉”营销公司提供的资料显示，其在引流吸粉的同时，也可售卖技术，“爆粉机器人软件500元一套，包括一年内的售后和使用。”也有营销公司表示，若花更多的钱可以提供教程、专业定制服务和对接的合作人士，“创建你自己的品牌”。

黑产“分身”上下游：上游想套路，下游行诈骗

李柚告诉记者，在引流中有一个流行说法，要想出套路来比你会技术重要得多。“五年前是你怎么样通过各个平台限制进行引流，现在通过平台限制已经交给整个外挂生产供应商来解决，上游想套路，下游想怎么诈骗就可以了。”

记者在调查中发现，目前绝大多数的引流产业的上游只提供引流服务，与下游实际上处于分开的状态。有业内人士指出，这是为了规避责任，“下游如果发生了诈骗或者售卖违禁品等违法行为，那么引流方就可以以不知情为由逃脱监管。”

据了解，目前引流黑产下游主要包括黑五类产品销售、色情诈骗和杀猪盘等。

腾讯发布的《电信网络诈骗治理研究报告（2019上半年）》显示，2019年上半年的诈骗类型主要包括交易诈骗、兼职诈骗、交友诈骗、返利诈骗、低价利诱诈骗、金融信用诈骗、仿冒诈骗、色情诈骗、免费送诈骗、盗号诈骗十大类。其中交易诈骗占比最高，达到39.6%。报告通过对诈骗社交场景下诈骗行为的分析，发现相当一部分诈骗行为源自多平台、跨平台的引流。其中二手交易平台、婚恋招聘网站、短视频平台出现诈骗引流较为突出。在电信网络诈骗实施过程中，人工智能开始被用于群聊群控场景，诈骗行为人制作聊天机器人程序，配合人工操作，将被害人引入迷局。

北京盈科（杭州）律师事务所方超强律师对记者表示，通过言语诱导等方式将不同平台的用户引流到微信号上的行为至少涉及虚假广告，“如果这一行为最终售卖的是正当商品，涉嫌营销手段违规，毕竟这属于虚假广告。而如果售卖的是淫秽物品或者进行诈骗，那么提供引流服务的也要作为同案犯被抓，因为哪怕只是商业上的委托关系，也提供了商务上的合作，对于淫秽物品的扩散是发挥了作用甚至主要作用的。”

记者发现，不少以营销为名成立的引流公司往往会以“技术中立”掩饰自身的黑灰产身份。对此，方超强表示，推广技术中立也需要看道德立场以及具体情况，“技术中立不是免责的理由”。

安全人士：黑产迭代对抗监管，需进行系统化打击

记者发现，在对抗引流黑产上，平台的各种封禁规则是第一重防线。

2019年12月20日，腾讯公司高级法律顾问钟萍在北大E法论坛上表示，针对在平台内发广告等引流行为，企业通常会对这些恶意账号和行为进行账号封禁等处罚，而在恶意营销外挂的帮助下（低成本发起大量攻击），网络账号被引流团伙充当消耗品，可以利用大量身份信息不断注册新的账号。这些恶意账号消耗着企业提供给正常用户的资源。另一方面，识别和处置这些恶意账号和行为，对企业来说是巨大人力物力成本。

钟萍称，黑产的这种上下游配合模式使得打击难以到位：大量行为处于灰色地带，网络黑产上下游分级，打击外挂时，相关团伙多数会以不知道设备将被用于恶意攻击为借口躲避。而相关上下游打击较少的情况下，网络黑产对于营销外挂的整体需求不变甚至增加，都会致使外挂打击难度进一步提升。

根据腾讯提供的资料，营销外挂的供应商通常会伪装为正常硬件供应商，且偷换概念为管理软件的开发商，通常硬件设备和管理软件分离，受到打击后，可以将攻击软件短暂分离，以逃避打击。而且营销外挂的更新迭代速度非常快，通常每3到6个月就会进行软件版本的更迭，10到14个月进行一次硬件的换代。

12月20日，腾讯方面对记者表示，国内互联网公司对于网络黑灰产的打击存在一些可以改善的地方，主要包括：注重技术打击和刑事打击，忽视民事、行政打击的力量，导致大量黑灰产特别是灰产行为逍遥法外，灰产（工具类、账号类）打击力度不足；民事、行政打击碎片化，没有形成系统化的打击体系。

腾讯称，已经注意到黑灰产的野蛮壮大，目前已经发布“南极光计划”，作为国内首个通过民事诉讼、行政查处打击网络黑灰产的系统化行动方案。南极光计划主要包括四个方面的黑灰产打击：源头类、虚假流量类、恶意营销类、游戏外挂类。

“实际上，打击黑产不应分而治之，比如引流属于恶意营销类黑产，但引流需要的各个平台账号的注册就属于源头类黑产，如果只打击引流方面不打击源头方面，就会发现依然有源源不断的‘供应商’，封禁一家黑产，自然有另一家黑产代替此前的位置，所以进行系统性的打击才是行之有效的方法。”Adan告诉记者。

记者注意到，各大平台针对网络黑灰产的打击在逐渐加码，百度正式发布“光明行动计划”，京东金融自主研发了天盾账户安全与反欺诈系统。而针对账号源头类黑灰产、微信和QQ分别开展了“死水行动”和“绿萝计划”，2017年死水行动上线以来，微信的恶意注册量降幅达到50%，存量恶意号总量降幅达到60%-70%。

北京允天律师事务所合伙律师周丹丹表示，对于恶意营销外挂软件的司法打击路径，主要包括平台对关于外挂用户协议的规范，民事诉讼的打击策略，行政投诉方式打击策略和刑事报案方面的打击策略。在刑事的处理方式中，从群控行为的性质来讲，可以归入四个罪名当中，主要包括非法获取计算机系统数据罪，提供侵入非法控制计算机信息系统的程序、工具罪，侵犯著作权罪，非法经营罪。

“而行政投诉方面，主要是向国家版权局、打黑办或者文化执法大队进行行政投诉，但是目前来讲，我个人认为行政投诉并不会是一个特别有效的方式，因为群控对行政主管机关比较难以认定是否构成违法行为。”周丹丹表示。

（据《新京报》）