黑灰产业在新媒体领域的现状及应对

朱婧

中文摘要：随着社会的快速发展，越来越多的人接触新媒体、使用新媒体。各类新媒体平台在发展用户的同时，也有越来越多的黑产、灰产从业者在暗中窥视着一切。本文将从微信、短视频、薅羊毛盛宴几个角度出发，着眼于黑灰产的商业运营模式，分析黑灰产业在新媒体领域的蔓延现状并制定应对措施。本文的研究创新点主要是在于对案例的独特解读与分析。本文的研究期望是网民能够清楚地认识网络黑灰产并了解其套路，能够为网民提供更为干净的新媒体平台。

关键词：黑灰产业；新媒体；网络安全；个人信息

1. 黑灰产业
2. 背景

黑产指的是直接触犯国家法律的网络犯罪。灰产则是游走在法律边缘，往往为黑产提供辅助的争议行为。从互联网的黑灰产业的技术来看，主要涉及的技术领域包括操作系统开发、程序设计、漏洞挖掘、数据开发等。从市场来看，互联网黑灰产的主要市场集中在垃圾账号交易、身份信息交易、软件交易、电信诈骗等多方面，并且已经形成了具有明确分工的产业链。

流入

行使新人权利

注册账号

购买

1. 黑灰产业类型

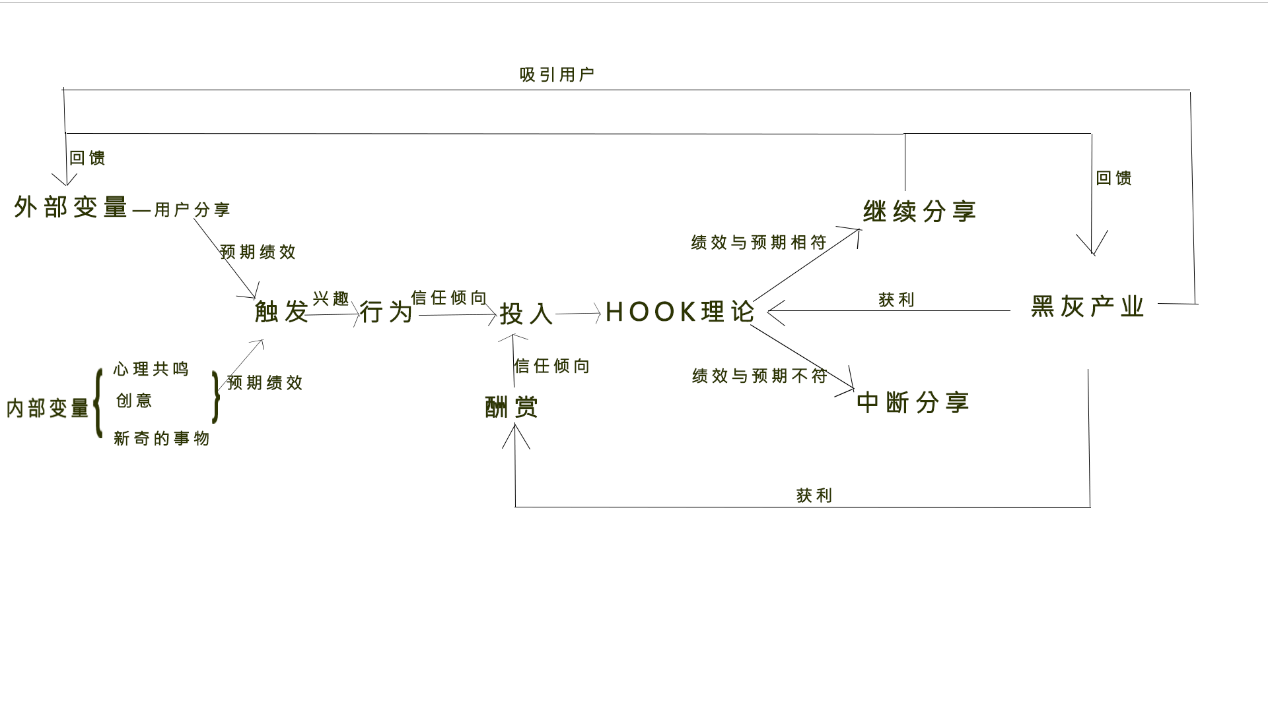
中国互联网的黑灰产业可分为四类：黑客技术、工具与培训产业链、真实资产盗窃产业链、网络虚拟资产盗窃产业链与互联网资源与服务滥用产业链。这其中的真实资产盗窃产业链是对公众威胁最大的产业链，因为涉及到银行卡账号密码的盗窃、电信诈骗等方式。网络虚拟资产则主要指网络空间中的资产盗窃，包括游戏账号、游戏资产等内容的盗窃。黑客技术和工具与培训产业链为资产盗窃产业链提供了技术支持，互联网资源与服务滥用产业链则给它提供了网络资源，最终获利的节点是真实资产与网络资产盗窃产业链。

1. 个人信息泄露是黑灰产的源头

在信息大爆炸的时代，个人信息泄露随处都是。尤其随着各类新技术、新业态、新应用不断涌现，手机APP、浏览器、社交平台、理财软件等，都有可能不知不觉间出卖信息。由于互联网账号体系的复杂性，每个人会习惯使用相似的账号密码来组合登录不同的网站，而各个网站的防控能力是存在高低的，所以黑客可以通过获取到的低风控门槛网站数据来进行碰撞以期获得账号的相关权限，这些都已成为恶意攻击者的常用手段。

1. 案例分析

我以微信公众号吸引用户为例，以HOOK为理论模型，对黑灰产业在微信中的获利方式和吸引用户方式进行了图解。



1. 微信：“2020年会发生的几件事”

前一阶段，微信朋友圈里被“2020年会发生的几件事”刷屏，本来我以为这就是一场平淡无奇的刷屏运动，每年到了年末的时候都会有类似这样回顾过去一年，展望新年的活动，参与门槛低，大家也都乐此不疲。这个活动能够刷屏的原因就在于：话题应景、参与门槛低、文案套路深。2019只剩最后一个月不到了，大家往往一边感慨时间过得好快，一边憧憬着新一年的开始。更何况，最近的刷屏新闻都是负面消极的，崔雪莉去世、刘阳出轨、宇芽被家暴、高以翔猝死……不好的消息一个接着一个，大家都在祈祷2019年快快过去，希望新的一年一切都好。这个话题的参与难度确实也非常低，全程只需要扫码参与、开始测试、出结果这几步，没有年龄、职业的限制。我仔细看了大家分享的结果，要不就全是好事，“吃饭有人约、某人把欠你的钱还清了、额外获得两天假期……”，即使未必会有好事发生，大家也愿意相信并分享出来；要不就是抓住了大众的痛点，“被催婚、工作、被表白……”，催婚、单身、为工作奔波等等都是这届年轻人经常挂在嘴边的问题，自黑文案刚好给了他们宣泄情绪的出口；还有就是搞笑风格，“吃吃吃吃、胖十斤、日渐消瘦……”，严肃不受欢迎，搞笑反而让人愿意分享，非常适合现在年轻人的发朋友圈风格。

然而这看似平常的刷屏活动，背后却是黑灰产的跨年大型轰趴。“2020年会发生的几件事”没有放任何品牌，因此它的目的不是影响力，而是引流。做完活动，想要退出的时候，它直接跳转到了一篇色情小说，通过小说来引流无非就是抛出一个章节作诱饵，到关键情节处戛然而止，想要获得更多内容，需要关注公众号才能获取。有朋友说他测完直接跳转到了算命的界面，填写个人信息即可获得初始测算结果，如果它引起了你的兴趣，那就得加个人微信号付费咨询。

本以为只是一场普通的营销活动，原来背后是黑灰产的年底大轰趴，而且仅仅我的朋友圈就有很多人参与了活动，其实我们都在默默地为黑灰产引流“贡献”力量。

1. 短视频：有流量的地方就有利益

曾经红极一时的直播答题，影响力极大，甚至连人民日报都为它发文点赞，更是为短视频平台带来了一个里程碑式的起点去年年初，随着“国民老公”王思聪的一条微博将一款名为“冲顶大会”的APP送上了热搜，“10秒答对12题，即可瓜分奖金”的游戏很快地传播了起来。一时间，众多短视频平台纷纷推出了芝士超人、冲顶大会等等，王思聪、张一鸣等大佬争当撒币侠。每天准点开放几道题答题，并附上高额的奖金，这样的噱头为各大短视频平台带来了将近百万的高活跃用户。身为庄家的众多平台，看到群众如此高涨的情绪，怎会就此收手？而趁乱潜入“白嫖”巨轮的黑产人士，怎会袖手旁观呢？

就这样，这个为了带动短视频、直播平台的资本催熟游戏，很快就遇到了开挂玩家。一次性答对12题并不容易，所以平台允许以此复活机会，复活机会可以通过平台活动或者是邀请新用户来获得，这就达到了平台拉新人的目的。

黑灰产从业者从根源上出发，卖题库、卖答案，如果不想背答案就填写好友邀请码。与刷粉的形式很像，创建无数个小号。没多久就出现了使用fiddler刷复活卡的方法，但一天之内也就失效了。三天后，出现了各类答题助手和各个平台注册工具。在各大答题直播平台上实测，这个工具2-3秒就能出答案，并且该工具还连接了人工，降低了AI搜索造成的错误的风险。

根据互联网参与者的需求，黑灰产的服务一应俱全，从账号商人、工具开发者到代理IP平台、接码平台，每一层都有成熟的利润获取方式。

1. 薅羊毛盛宴

“薅羊毛”是指搜集各大电子商城、银行、实体店等各渠道的优惠促销活动、免费业务之类的信息，用零成本换取物质上的实惠。

年初，拼多多出现了严重漏洞，任何用户都可以随意领取100元无门槛优惠券。有专职“薅羊毛”的人发现了这个漏洞，大肆传播。

实际上，在电商平台上类似的漏洞并不罕见。

不久后，小米旗下的米家有品商城出现了价格漏洞，原价599的商品只需要0.01元就可以购买，消息传开后引发网友第一时间疯狂抢购。

双11期间用梦洁谈毛天猫旗舰店发放的满减优惠券消费后，商家迟迟不发货。梦洁的售后解释称“优惠券是系统错误导致的。”

东方航空也因为系统维护时出现漏洞，全国各地往返的头等舱、商务舱和经济舱均出现1折以下的超低票价。

这些都是网络黑灰产团伙通过寻找一个漏洞来盗取千万元平台的优惠券，进行不正当牟利。有法律人士表示，在“合理自用”范围内，普通用户使用平台的某一有漏洞的优惠券，从法律实践来说，会被认定为是平台的促销。但对于重复注册账号、使用网络漏洞等方式来使用这一优惠券的，如果证据确实，恐会涉及不当得利乃至非法侵入计算机系统等刑事罪名。有安全专家指出，一般情况下，优惠券会设立领取门槛，结合登录IP、账号等，以此来避免一些人士利用虚拟设备批量“薅羊毛”。而上面的拼多多事件并未涉及虚拟设备，大量用户都是使用常规设备领取并完成交易的，直接原因可能是平台的风控体系欠缺并且能力不足。

1. 应对措施
2. 网民们要提高安全意识

网民们需要提高自己的安全意识，一是要保护好自己的隐私，二是要学会使用安全工具保护设备和应用的安全，从正规渠道获取应用，杜绝个人设备被黑灰产利用。

提高个人的安全意识，包括不去点击各类社交媒体中流转的信息和地址链接，现在多中木马都是通过社交媒体在进行广泛传播，传播的媒介包括各种可执行文件、压缩包、文档等等。而且网络黑灰产会借助社会热点来进行传播，所以在点击之前一定要确认其是否安全。此外保护个人隐私，不轻易向他人泄露个人信息，不能轻信任何客服电话、银行电话，绝不向别人泄漏个人账号密码和身份证上的信息。

学会使用安全工具保护设备和应用的安全要求我们在手机、电脑等硬件设备中安装安全软件，保护设备免遭病毒和木马的攻击，并且要经常更新，减少风险。安装各类软件的时候要从官方渠道或者各大应用市场中下载，不要轻易相信来自网盘、论坛等的软件资源，对破解版要保持警惕，提升手机、电脑等的使用安全。

1. 企业要提高自身安全建设能力

企业要提高自身的安全建设能力，像滴滴、小米、拼多多、腾讯等平台，都保存着众多用户的信息，不断提高平台的安全防护能力，防止出现大规模用户信息泄露是斩断黑灰产业生产资料来源的重要工作。

要借助互联网企业提供的安全防护能力来构建自身的安全防护能力，如使用腾讯云、阿里云等云平台，借助云盾等云安全产品与服务来提高自身的安全防护能力，防止以内安全防护能力不足所造成的信息泄露问题。

对于众多互联网创业公司，在产品的开发过程中，会出现创业公司常见的因开发不规范造成的漏洞与问题。Software Development Kit可以大大提高应用端的安全。

1. 政府要加快立法并实施

随着我国信息化进程的高速发展，社会公众对健全法律体系、保障自身利益的需求也随之不断提高。2009年《刑法》修正案增加关于网络犯罪的条文，对入侵计算机信息系统犯罪和提供相关工具的行为进行了定罪。

2009年，最高人民法院和最高人民检察院新增非法获取计算机信息系统数据罪，非法控制计算机信息系统罪的相关解释。

2012年，全国人大发布《关于加强网络信息保护的决定》。

2015年，工商总局发布《侵害消费者权益行为处罚办法》。

……

在颁布了相应的法律法规之后，我们还需要有具体的判例作为参考。针对不同的主体均有依据网络安全法的相关违法行为的监管动作，其中包括对互联网企业腾讯微信、新浪微博、百度贴吧涉嫌违反《网络安全法》的立案调查等。法律实践解决了两个问题：让公众对网络安全的任职提升到新的高度，对个人隐私、数据安全以及各种网络诈骗行为有更直接的感知；为各级执法机构提供了非常明确的行为指导和判例指导，在类似的违法行为发生时，在处置和量刑上会有法可依，有章可循。

1. 总结

本文就是希望通过对一些典型案例的分析阐释，从而让大众更为清晰地认识网络黑灰产，并针对不同的群体提出不同的应对措施。最终的期望是虚妄不断增加黑灰产业从业人员的违法成本，从技术上提高作案难度，大众的防范意识与防范措施的不断增强，各平台的防范能力不断提升，监管部门的识别能力不断提升，并且在法律法规的不断完善下能够有明确的监管执行措施，让灰色产业的违法成本不断提升，最终远超过其违法收益。在这背后带来的，将是对网民们而言更少的垃圾信息、电话的骚扰，拥有更加干净的网络环境，给新媒体平台更加公平、更加纯净的发展空间。

1. 参考文献
2. 于冬. 中国黑客灰色产业链调查【J】. 政府法制,2009(21):41-41.
3. 王新. 网络黑色产业链问题成因及对策【J】. 商业现代化,2008(12):276-277.
4. 杜跃进，李挺. 移动互联网安全问题与对策思考【J】. 信息通讯技术,2013(4):11-13.
5. 作者简介

作者姓名：朱婧，就读于苏州大学传媒学院2018级网络与新媒体专业，任班长，研究方向：新媒体安全。