

起底“羊毛大户”

组织严密轰炸式抢占优惠 “羊毛党”变身“饿狼党”

新华社 何曦悦 谭慧婷 王默玲

什么是“薅羊毛”？这一名词远不止在电商平台找优惠券、抢到“0元购”商品那么简单。近日，电商平台“拼多多”出现百元优惠券漏洞被大量“薅羊毛”，敲响了防控大数据黑产业的警钟。组织严密的黑灰产业链条，先进技术手段攻破平台风控防线，百万元级利润收入……“羊毛党”是如何变成有组织的产业并日渐壮大的？他们对互联网产业的健康发展带来了怎样的危害？记者就此进行了调查。

拨开“羊毛圈”：“只有你想不到，没有我薅不到”

90%的冰山在海面以下。记者进入了一个“羊毛群”，发现这里仿佛是另一个世界：一些忙着往群里扔“福利”的“大V”，几百个每日蹲守群里接福利的“羊毛客”，不断被朋友拉进群的“小白”……他们有自己的网站、论坛，平时会交流心得、总结经验、分享“线报”。

从各大网站“BUG价”“秒杀价”，到P2P、区块链、小额借贷等平台的注册金，如今“羊毛客”们又大量回归并专注于电商平台以及微信公号福利。记者在一个专注某电商平台福利的微信群里看到，群主在5个小时里发布了98条“线报”，主要集中在商品秒杀、领券等优惠信息，同时也有试玩App等花样繁多的“刷单”式羊毛。记者在一位“羊毛客”的指导下尝试下载某App并按要求停留3分钟，果然收到了

0.16元的“赏金”。网友“看夕阳落下”称，自己“人行仅一个月，就已经赚了5000—6000元”。

但这只是“薅羊毛”的入门级操作。从蝇头小利中不断累积的“羊毛客”，渐渐发展成拥有大量资源和专业设备的“羊毛大户”。据介绍，“羊毛大户”们大多“积累了大量身份资料，有可靠的关系网络收集线报，有程序员功底”。这从“拼多多”网站在凌晨出现优惠券漏洞，随即被迅速领取数千万元的案例中可见一斑。

据群内“羊毛客”介绍，“邮币卡火的时候，某大牛一高兴直接提了宝马3系”“某大牛单每月的理财收益就有8000元以上”，如今“行情不好，很多网络项目也被封杀殆尽，许多大牛的公众号也被封杀”。但“大户”依然存在，并正在借用更高级的科技手段，成为活跃在互联网平台背后的一群“黑色阴影”。

探寻“羊毛头”：手握万号抢优惠 狠钻空子建黑产

在“羊毛党”的圈子内，不少骇人听闻的案例被传为“美谈”：某上市公司用现金激励推广直播软件，但10亿元以上的主播奖励大部分被“羊毛党”以黑卡套走；某电商平台发放“满2000元减50元”优惠券漏设使用门槛，有“羊毛党”一人就狂刷1.7万单……

“羊毛党”何以能短时间内攻击并“薅”垮一家平台？业内人士揭露，“薅羊毛”三字背后是巨大的黑产圈。

网盾易盾业务安全产品专家刘庆介绍，近几年越来越多的企业开展“撒钱”吸引新用户、拉流量的活动，着实养肥了不少黑产业的腰包。黑产业分工也愈发精细，并不断利用新兴技术手段。

“新用户优惠”拦不住“羊毛党”的步伐：黑灰产人员或是拥有多达数十万乃至千万级别的手机黑卡库，或是利用“接码平台”的大量卡号资源，以每条0.1元左右的价格接收验证码，快速并大批量注册。高级的验证码技术有时也难以形成防控机制：“羊毛党”利用“打码平台”的人工智能技术，以机器、人工结合的方式识别各种图片验证码。2017年，绍兴警方就曾通报其破获的“快啊”打码平台案件，该平台3个月内就提供了验证码识别服务259亿次。

《阿里聚安全2016年报》记述了大规模“羊毛党”的危害：互联网上缺乏安全防控的促销、红包活动中，70%—80%的优惠都会被“羊毛党”薅走。大规模的批量机器下单，甚至能够造成网站瘫痪。

面对“羊毛党”来袭，此前有电商平台紧急召回已发出的货物；有知名咖啡品牌紧急叫停赠饮活动。但经验丰富的羊毛党大多掌握专有“洗白”渠道，青睐高流通性的话费、Q币等产品，一旦变现就难以追回，很多平台不得不“吃哑巴亏”。

“饿狼”扑“羊毛”：从卡号到企业亟待建立安全网

掠夺网络资源、参与流量造假、逼停创业公司，“羊毛党”更像是一群“饿狼党”。

事实上，他们的行为已不再只是游离于违法的边缘。

上海明伦律师事务所高级合伙人赵陆一律师表示，通过购买、交换或网络下载等方式获得私人手机号码等个人信息，用以在网络平台注册换取首单优惠等，就构成了侵犯公民个人信息罪；而“羊毛党”通过不正当途径获取大量平台优惠券，则可能面临盗窃罪的处罚，各地量刑标准不同，在上海累计达到1000元就构成盗窃罪。

深探“黑产业”背后，他们抢占优惠的大量手机卡号究竟从何而来？中国信息通信研究院产业与规划研究所副主任杨天一介绍，除了实名注册的国内手机卡，境外手机卡等，根据业内机构的调查，目前流通的手机黑卡中80%以上是物联网卡。

杨天一表示，手机黑卡的平台化趋势亟须管控。除了进一步细化对手机实名制管理的规定，还应针对电信运营商号卡建立体系化管控机制，特别是针对物联网卡等新类别的号卡，最好采用专门号段，更要加强号卡供应商的资质审核和管理，严禁层层转售。

专家认为，一方面，对于企业来说，升级风控体系成为必要选择。刘庆介绍，由于黑灰产业群体应用的技术手段非常多，因此企业需要使用更多数据维度和指标，构建更复杂的策略、模型进行防御。另一方面，要整合互联网安全企业资源，形成有效的系统化合力。杨天一建议，建立共享的黑卡数据库，并鼓励社会力量参与，为进一步加大对黑卡的精准打击等提供支撑。

“指尖经济”助脱贫



制贩毒品超3吨

重庆两主犯一审被判死刑

新华社 周闻韬

近日，重庆市第五中级人民法院对胡进来、胡文武等18人贩卖、制造毒品案作出一审宣判，胡进来、胡文武被判处死刑，剥夺政治权利终身，并处没收个人全部财产；胡国兴、陈伟宾被判处死刑，缓期二年执行；其余14人分别被判处六年至无期不等的刑罚。

经法院审理查明，2016年12月起，被告人胡进来和胡文武开始共谋制造毒品谋取非法利益。2017年1月，胡文武

安排人员在四川省乐至县境内联系制毒场所、人员，购置制毒工具、辅料等，后因怀疑被村民发现而逃离。同年2月初，胡进来、胡文武安排胡国兴到重庆境内寻找制毒场地，将制毒地点确定在位置偏僻的重庆永川区红炉镇附近。

重庆市第五中级人民法院审理认为，被告人胡进来等人共同制造毒品氯胺酮约1200千克，胡进来、胡文武在制毒过程中起组织、指挥作用，此外，胡进来、胡文武还伙同他人非法买卖、运输制毒物品羟亚胺约2000千克。二人在

贩卖、制造毒品的犯罪中系主犯，其行为均已构成非法买卖、运输制毒物品罪，且属情节特别严重。公诉机关指控的事实和罪名成立，应依法数罪并罚，法院遂作出前述判决。

手机网络买保险 赢客户节大礼

官网投保 **epicc.com.cn**

电话投保 **400-1234567**

PICC 中国人民保险

134个恶意程序藏身短信 窃取用户个人信息

新华社 周润健

春节将至，很多人会收到各种邀请函和请帖等手机短信，不过这时候一定要擦亮双眼，因为有些恶意程序会藏身其中，伺机窃取你的短信内容和通讯录，对你的信息安全造成威胁。

记者23日从国家互联网应急中心天津分中心获悉，通过自主监测和样本交换形式，国家互联网应急中心近日共发现134个窃取用户个人信息的恶意程序变种。

这134个恶意程序变种名称包括QQ刷赞大师、年会邀请函、微笑者专业盗号、违章查询CW、移动积分兑换、招标文件、宅男宝盒、厘米秀刷花神器、聚会报名同学录等。这些恶意程序目前已攻击影响了四川、河南、福建、广东、山东、河北等地用户的手機。

国家互联网应急中心天津分中心安全专家介绍说，被曝光的这134个恶意程序主要危害涉及：私自将用户手机里已存在的所有短信和通讯录上传至指定的邮箱；私自接收指定手机号码发来短信控制指令，执行控制指令内容；私自将用户接收到的新的短信转发至指定的手机号码，同时在用户的收件箱中删除该短信。

为避免个人信息被恶意程序窃取，安全专家提醒说，对于无缘无故出现的链接或文件，尤其是陌生用户通过短信、微信等工具发送的链接或文件，不要点击或接收；手机上的重要信息如通讯录，需要定期备份，并且要限制各类App的访问权限。同时，在使用手机观看视频或浏览信息时，不要点击如一夜暴富、轻松赚钱、色情、赌博等广告链接。另外，打开手机中防病毒移动应用的“实时监控”功能，对手机操作进行主动防御，这样可以第一时间监控未知病毒的人侵活动。