黑镜调查

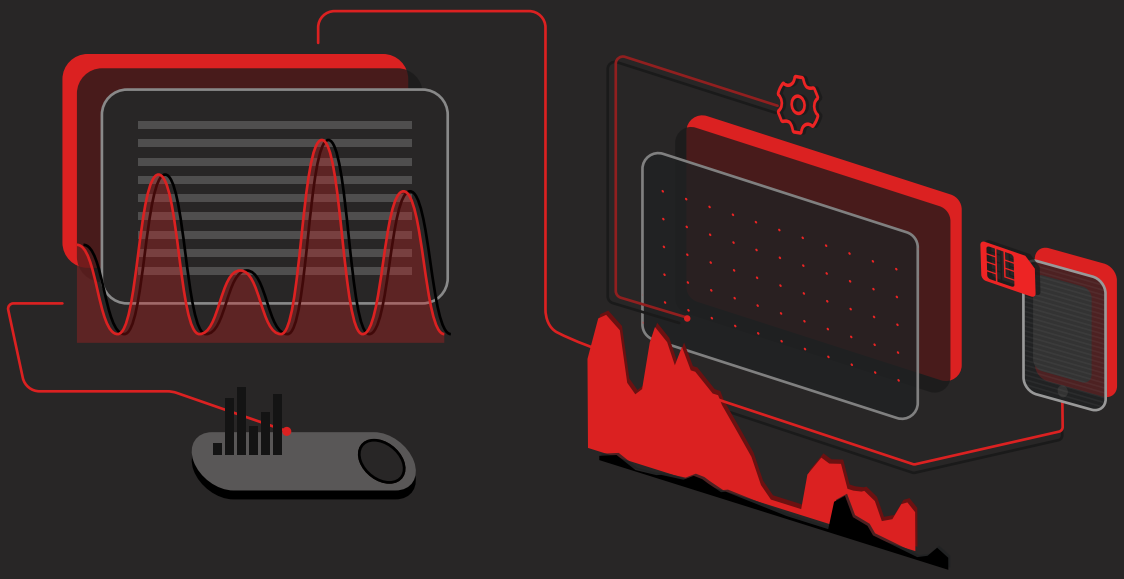
深渊背后的真相之「薅羊毛产业」报告

同盾科技 www.tongdun.cn
FREEBUF WWW.FREEBUF.COM

声明

本报告为FreeBuf与同盾科技联合研究成果。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。

关于同盾科技

同盾科技有限公司成立于 2013 年，总部位于浙江杭州，是国内专业的第三方智能风险管理服务提供商。自创立以来，同盾始终坚持“跨行业联防联控”的理念，将人工智能与风险管理深度结合，为非银行信贷、银行、保险、基金理财、三方支付、航旅、电商、O2O、游戏、社交平台等多个行业客户提供高效智能的风险管理整体解决方案。

数据及内容支持

漏洞盒子　　同盾科技反欺诈研究院

目录

目录

第一章 概述

1.1 内容简介

这是最好的时代，只要能上网，每个人似乎都能恣肆张扬，找到存在感，在网络中一次次地集体狂欢；这是最坏的时代，网络连通一切，带来的虚无感让很多人沉溺其中，忽略甚至忘记了现实世界的规则。

根据 CNNIC 2017 年 7 月发布的《第 40 次中国互联网络发展状况统计报告》，截至 2017 年 6 月，我国网民规模达 7.51 亿，中国手机网民规模达 7.24 亿。[1]如此大规模的数量预示着大量的网络需求；而如此大规模的流量一旦变现，就意味着庞大的利润。随着技术飞速发展、信息传递越来越便捷，主流互联网产品和服务之外又围绕着“流量”衍生出了一条条地下产业链。这些产业链将越来越多的流量吸附进去，逐渐形成了一个个深渊。

本报告就从其中的“薅羊毛产业链”入手，借由同盾科技的智能风控引擎所捕捉到的数十亿风险行为数据，以及深入调查几十个薅羊毛 QQ 群，接触几千名 QQ 群成员，通过数据分析、真实调查等方式，解读如今让商家避之不及的“羊毛党”团伙运作流程，并揭秘依托 QQ 群发展的羊毛党真实故事。以期让业内对当今薅羊毛产业有整体、直观的了解，并通过真实案例展示企业在技术或业务逻辑上存在的、易被黑客利用的漏洞，借以提醒企业、项目管理者在产品或业务中重视安全问题，并给予相关决策者一定的参考和指引。

同时，在调查过程中，本文还发现这条产业链背后存在着深刻的社会问题，对我国教育、普法、社会监管等多个领域都有一定的警醒意义。

1.2 重要发现

1	薅羊毛行为已经从单人发展到群体化、规模化，形成了薅羊毛团伙和一条完整的产业链，并且呈现出全网流窜的趋势
2	2017 年前三季度，羊毛党的主要集中领域为各大娱乐平台；符合我国近年来以知识产权为核心的网络娱乐应用新兴商业模式迅速增长的互联网发展趋势
3	薅羊毛的攻防技术已经涉及到人工智能、生物认证等前沿科技
4	2017 年前三季度，企业平均每天遭受 241 万次薅羊毛攻击；前三季度薅羊毛总数超越过去三年的总和，造成的损失在千亿级别
5	2017 年前三季度，约有 110 万个薅羊毛团伙在互联网中“兴风作浪”
6	一部分羊毛党以 QQ 群为依托，也发展出一条 QQ 群薅羊毛产业链
7	薅羊毛 QQ 群成员中以 90 后和 00 后居多，他们本应专注于学习，却沉迷于薅羊毛；这反映出我国教育、普法等方面的问题
8	薅羊毛 QQ 群成员中男女比例特征明显：男性 QQ 用户更爱薅羊毛
9	薅羊毛 QQ 群成员在广东、山东、河南等人口大省或外来人口大省分布较多，表明我国在这些地区的社会监管的力度和广度都有待提升
10	企业应当引起警惕，使用合适的安全产品和安全服务

第二章 薅羊毛的概念与发展

2.1 薅羊毛的由来与概念

看着春晚长大的网友对于“白云和黑土”应该都是耳熟能详了。1999 年，宋丹丹和赵本山在央视春晚舞台出演了一个小品——《昨天、今天、明天》，在小品中，宋丹丹饰演的白云利用自己给生产队放羊的便利条件，揪羊毛搓毛线，给老板黑土织了一件毛衣。当时，节目中将这种行为戏称为“薅社会主义羊毛”。后来随着经济的发展，在各大线下线上活动中利用优惠活动等获取利益的群体就被称为“羊毛党 ”。

如果按照小品中对薅羊毛的定义，其实我们每个人或多或少都薅过羊毛。毕竟生活中的衣食住行用，多少都要涉及到商家的优惠。不管是打车时用的优惠券，还是餐厅的满减活动或者是商场的打折活动，都属于这个范畴。不过普通人的这种薅羊毛，并不会为商家带去很大的损失。商家反而很欢迎普通消费者来参加这种活动，一方面能推广自己的业务，另一方面也能够积累客户量，增长日活。

在风控领域，对羊毛党的定义则比较多样化。概括表述为：热衷于参与各种营销活动（包括但不限于：满减、返现、抽奖、优惠券等活动）的用户，但并不能给平台带来实际的活跃用户增长。还有一些羊毛党把薅羊毛当做职业，利用商家或者平台的漏洞，来大量攫取利益，甚至进行诈骗，对商家造成的损失以及带来的社会问题更加严重。

2.2 薅羊毛的发展历程

如果在百度中搜索“薅羊毛”三个关键字，大约能找到 700 多万条搜索结果。而页面旁边的推荐词，大多与理财 APP、金融产品，以及京东等电商平台有关。大量的广告页面中，只有一两条是防范羊毛党的产品广告，其余大多是推广薅羊毛的平台。

其实早在“羊毛党”这个名词出现之前，就已经有一些薅羊毛的活动了，主要是热衷于电商优惠活动的“淘宝客”，热衷于网络调查、打码、答题的“网赚群体”。在 2014 年之前，“网赚”这个词还比较热门，很多大学生参与网赚而被骗。

2014 年起，电商、团购通过微信进行推广促销，由于电商本身根基雄厚，活动形式简单、门槛低，微信红包、优惠券、满减、免单之类的推广活动几乎是零风险，迅速受到羊毛党的关注，使得羊毛党人数爆发式增长。相比之下，P2P 行业在这个时候才刚刚迎来发展的机会，要求实名、绑定银行卡，涉及到小额投资，直到 2014 年下半年，才开始被羊毛党“重点关注”。而此前的网赚群体，就在这个大潮中，成为了最早的一批羊毛党。此外，网赚群体中的小部分人，开始建立了博客、工作室，组建起具有一定规模的 QQ 群，YY 频道，为羊毛党提供活动线报、经验，同时也积累了大量的下线。这些渠道成为了日后 CPS 推广平台的主力。

2014 年下半年，是 P2P 行业的爆发期，也是羊毛党的发展期。起初的羊毛党都比较规矩，并没有像今天这样如狼似虎。他们掌握的信息资料（四要素信息：姓名、身份证、银行卡、手机号）很少，大部分可能来自于亲戚朋友，薅羊毛的过程中也很少使用作弊工具。而对实名要求不高的电商平台，依然是羊毛党的首选。并且，随着国内接码平台的出现，为羊毛党提供了充足的手机号资源，使得一个用户可以拥有多个账号，享受多次优惠。

到 2015 年，围绕“薅羊毛”产生的产业链，已经初具形态，上游有多家接码平台在提供手机号，针对各大平台的自动注册机、扫货机也开始风靡。并且出现了专门倒卖四要素信息的团伙，不少羊毛党都持有多套资料。羊毛党也开始出现了比较明显的分化，呈现出较为明显的分界线。拥有大量资料、愿意进行投资的羊毛党，专注于 P2P、理财平台的各种活动；而不愿意进行投资的的羊毛党，开始工具化、批量化在其他行业中四处掠夺。

各大薅羊毛的网站、论坛、公众号、QQ 群，CPS 推广，也是产业链中的重要一环。平台为了吸引活跃用户，获取到投资，往往会和广告公司或者 CPS 推广公司合作，平台按照用户的注册数量来进行费用结算。而广告公司和 CPS 公司在短时间内难以达到平台的预期，就会选择跟羊毛党合作，也就是找“刷子”。

此后，某些资深的 P2P 羊毛党，转变成了“刷手”，俨然已经成为他们职业。广告公司或 CPS 推广公司如果和“刷手”联手，会支付一定的佣金，佣金比例与刷手投资的金额成正比。举个例子，某 CPS 公司为了完成引流指标，寻找了大量刷手，根据注册量、投资金额、投资期限等计算佣金。而某个刷手使用多套资料注册了账号，每个账号上进行一万元的投资，期限为一个月，收益约为3%，同时还能够从 CPS 公司那里获得一定的佣金。

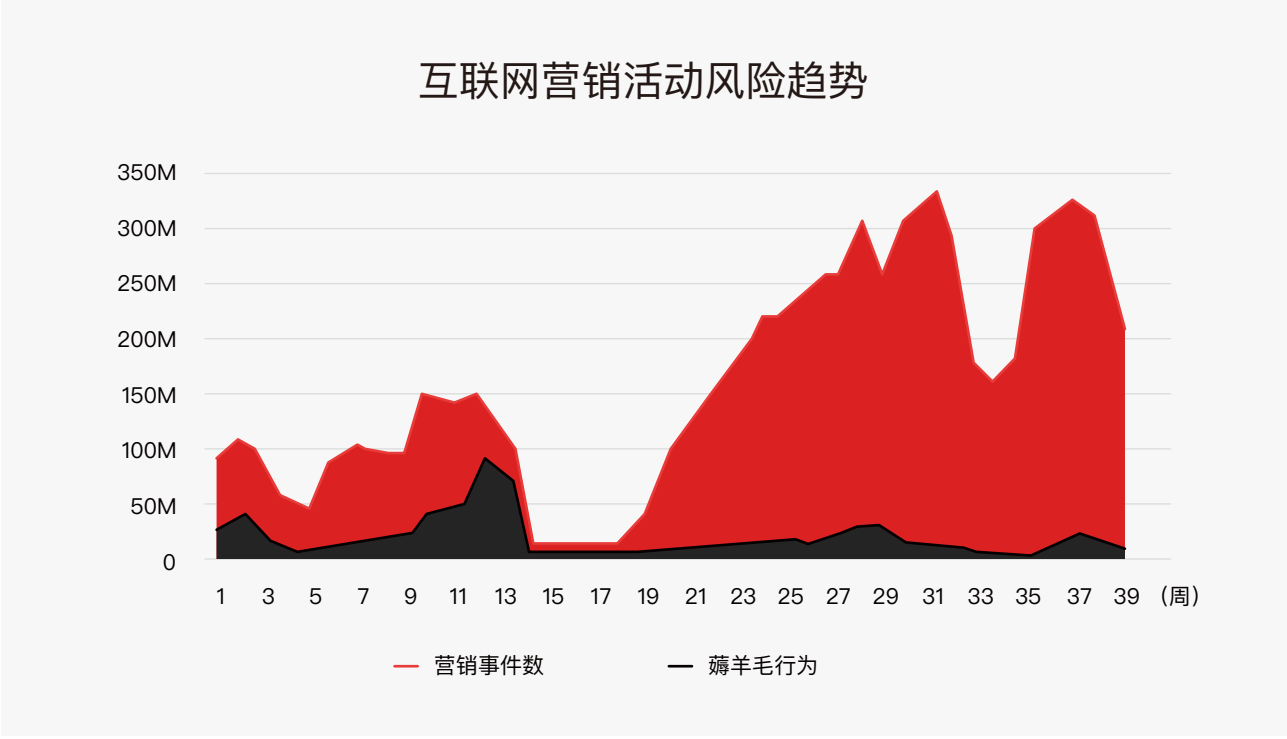
自 2016 年起，互联网金融面临严格的监管，卷钱跑路的 P2P 公司也有不少，对 P2P 羊毛党来说，最担心的莫过于平台跑路。而且，随着 P2P 市场格局趋于稳定，活动数量减少，推广的力度也下降很多，P2P 羊毛党也开始寻找其他的方向。

第三章 薅羊毛现状分析

时至今日，薅羊毛已经不再是原先的小打小闹，而变成了一场旷日持久的对抗。羊毛党在互联网上肆虐，犹如蝗虫过境一般，规模空前。

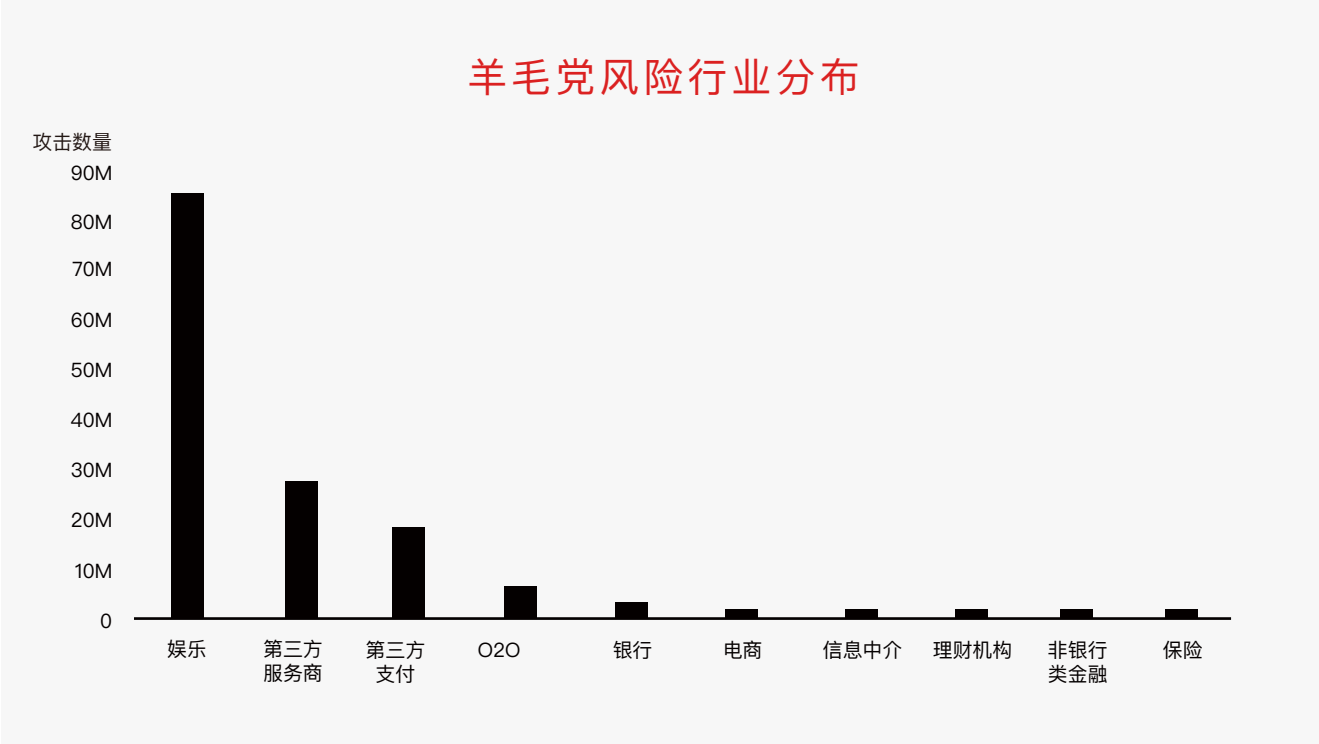
3.1 行为分析

根据同盾科技智能风控引擎在 2017 年前三个季度的统计，累计监测到超过 6 亿次薅羊毛行为。



其中，3 月份为薅羊毛爆发期，累计监测到 2.55 亿次羊毛行为，受影响的主要是第三方支付平台。

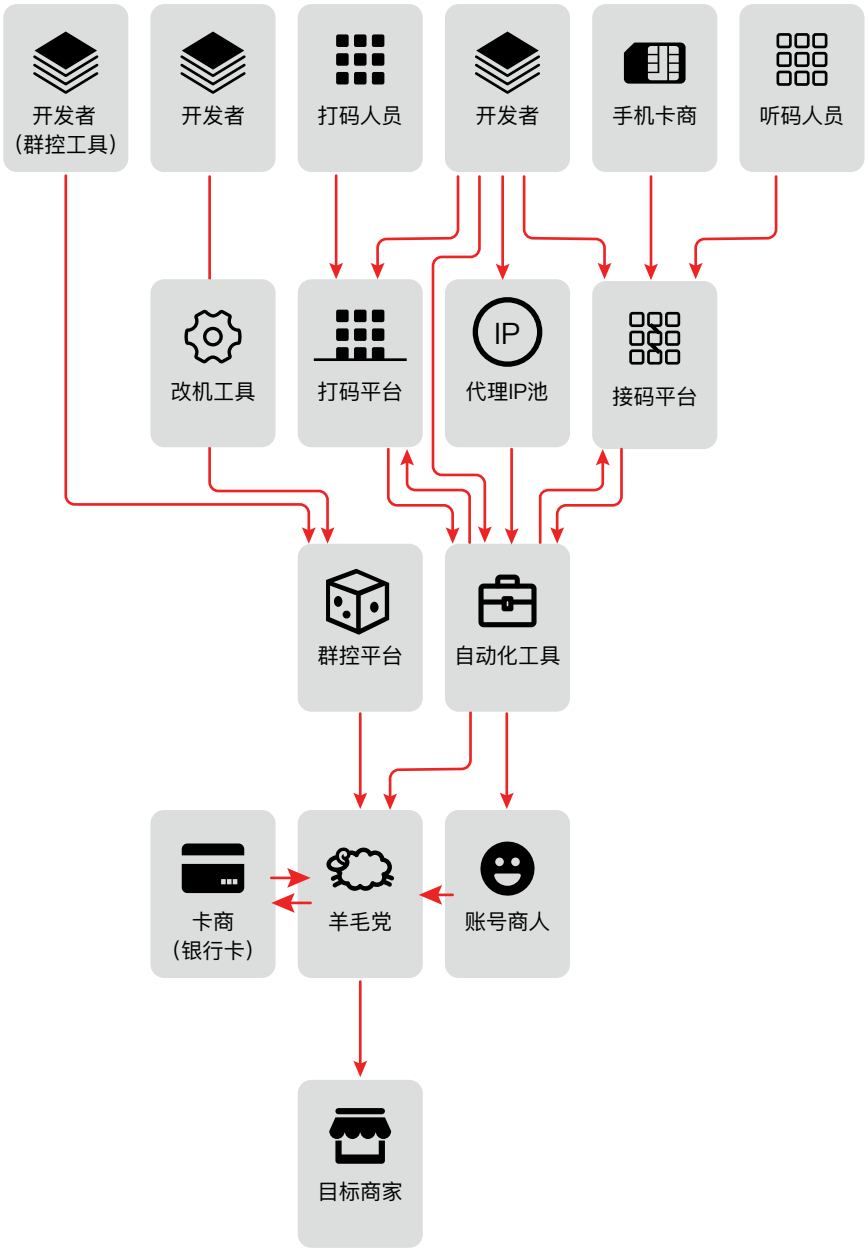
纵观 2017 年的前三个季度，羊毛党的主要聚集地，当属各大娱乐平台。譬如，直播平台、视频网站。



各大平台都采取了措施来抵御羊毛党，通过引入机器学习、业务蜜罐或第三方风控服务来保护自己的业务不受侵害。政府、公安、运营商等社会各界也在这场对抗中投入了巨大的力量。但这并没能阻止羊毛大军的脚步，2017 年过去的几个月中发生的薅羊毛事件，数量上超过了过去三年的总和。由此带来的经济损失，也是非常巨大的。

3.2 产业链分析

过去的几年间，羊毛党已经发展成为一只庞大的力量，薅羊毛过程中需要的各种资料、手段、工具，促生了上游的各种灰色产业，比如：接码平台、商业化的注册机、群控系统、代理平台、资料商人和账号商人，整个薅羊毛的产业链的结构，大致如下：



下面，我们来逐一分析这个产业链中各个环节。

3.2.1 手机卡商

手机卡商，属于整个产业链最上游的群体。数量众多的卡商们，为各大接码平台源源不断地提供手机卡，也就是风控领域中常说的“虚假号码”。

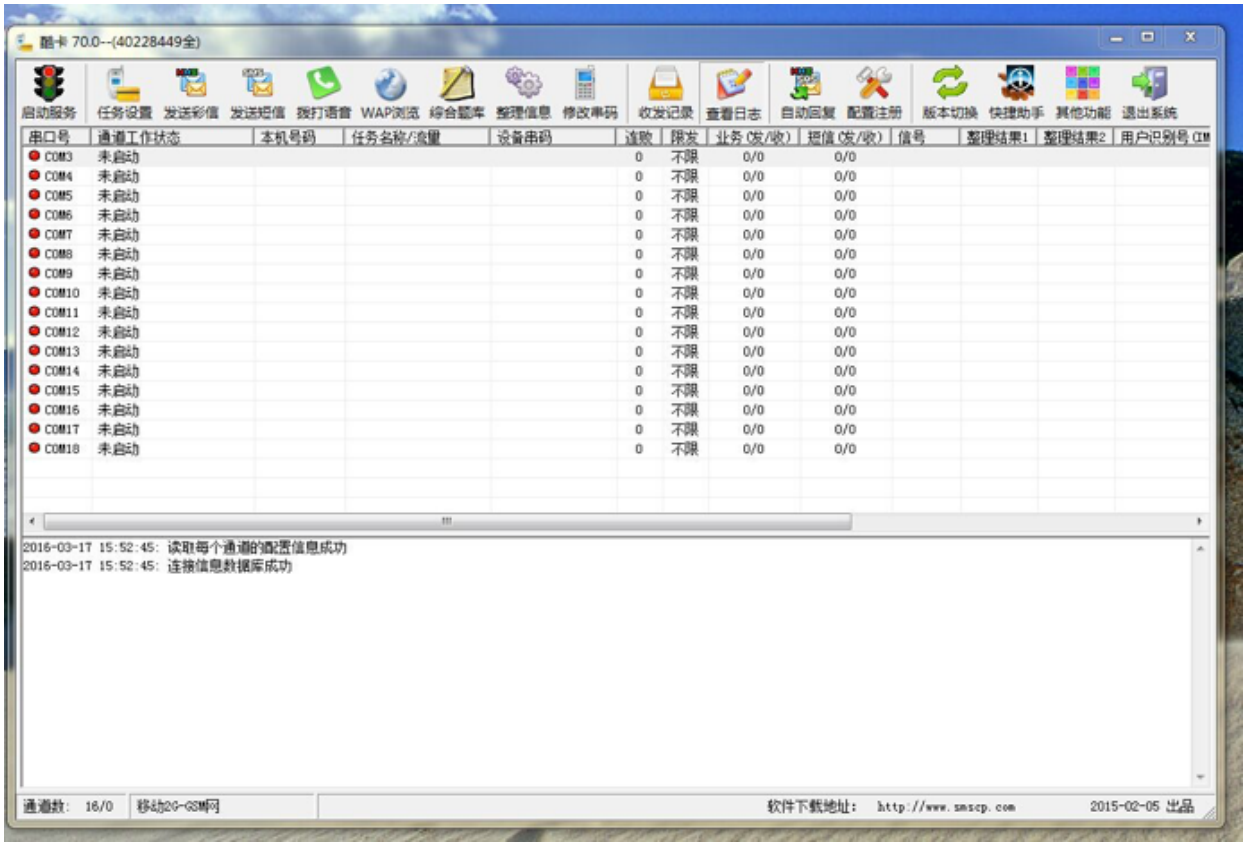
“虚假号码”并不是“虚拟手机号”（由虚拟运营商负责发行和管理的手机号），“虚假号码”泛指所有用于代替他人接收验证码的手机号。绝大部分虚假号码，没有经过实名制登记，存活时间有限，超出运营商规定的实名制期限，就会被强制停机，然后变成空号进行回收，再继续投放市场。也有部分虚假号码，是经过实名制登记的，可以长期使用，但随着时间的推移，这些号码被使用的次数越来越多，过往的风险行为很容易被识别出来，进而被标记为黑名单。

根据目前同盾反欺诈情报收集到的信息来看，绝大部分的虚假号码，依然是运营商内部流出的。资源充足的卡商可能同时持有上百万张手机卡，较小的一些可能只有几十个。

卡商账号: b 电话: 15 QQ: 12 备注: 虚拟卡	1000	¥1.00	14个	1000	点击接入
卡商账号: 电话: 1 QQ: 6 备注: 实卡和虚拟卡	100000	¥1.00	20个	99749	点击接入
卡商账号: 33 电话: 15 QQ: 10 备注: 实卡	10000	¥1.01	35个	9872	点击接入
卡商账号: 电话: 185 QQ: 3 备注: 虚拟卡	10000	¥1.01	15个	9996	点击接入
卡商账号: 1 电话: 13 QQ: 8 备注: 虚拟卡	10000	¥1.01	16个	9929	点击接入
卡商账号: a5 电话: 13 QQ: 5 备注: 实卡和虚拟卡	10000	¥1.01	18个	10000	点击接入
卡商账号: 17 电话: 1 QQ: 3 备注: 实卡	100000	¥2.00	1个	100000	点击接入

某接码平台上的卡商信息

卡商需要使用猫池，配合猫池软件来让手机卡工作。目前市面上主流的猫池软件主要有酷卡、嘻唰唰等。以酷卡为例，猫池连接到 PC 上之后，通过软件进行管理，可以在软件中对手机卡进行管理，主要的功能包括：设置通道对应的手机号、自动读取短信、发送短信、拨打指定号码、批量设置呼叫转移等等。



酷卡软件接受的短信，会保存在一个mdb (Access 数据库文件)文件中，配合其他软件，就可以自动读取和识别短信验证码。接码平台会提供卡商客户端，用于读取酷卡数据库中的短信记录，并发送到接码平台。接码平台会自动完成卡商的费用结算，每完成一次短信验证码代收，平台从中抽取 20%~50% 的费用。

由于硬件的一些限制，普通 PC 最多能同时连接 32 个 USB 外设，猫池中每 4 个卡槽作为一个 USB-Hub 连接到电脑上，这对卡商所能持有的手机卡数量造成了一定限制，也可以接触一些外设来进行突破。目前市面上销售的猫池硬件，最大可以支撑 2048 张手机卡同时工作。

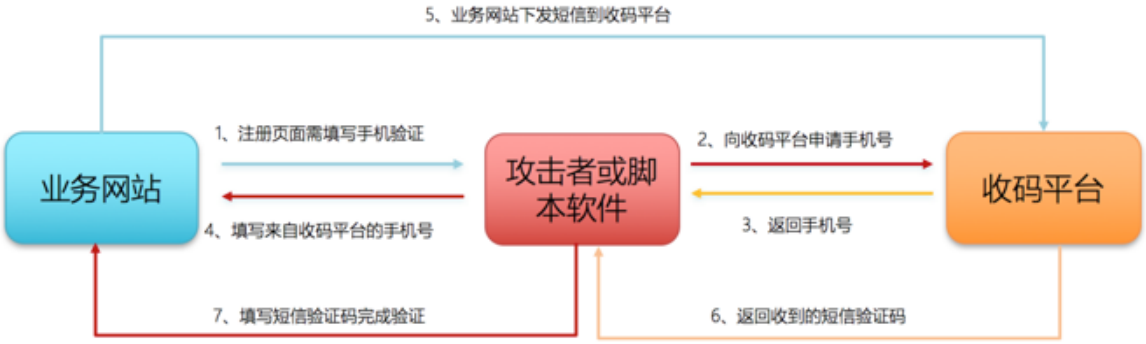
3.2.2 接码平台

2016 年 7 月份，浙江警方打掉了当时规模最大的接码平台——爱码，从爱码平台缴获了超过 700 万张已经使用过的手机卡。自此之后，接码平台基本上不再自己提供手机卡，而是全部由卡商来提供，平台在整个过程中，仅充当了羊毛党和卡商进行验证码短信交易的渠道。

接码平台一般会提供客户端、API，甚至手机客户端，服务端会根据预先设置好的短信模板对短信内容进行自动匹配，提取出其中的验证码信息，为羊毛党提供了极大的便利。

接码平台的 API，能够对接到自动化脚本和自动化工具中，实现批量化注册。

接码平台会提供两种形式的验证码获取。一般而言，用户先选择自己要注册网站，获取到手机号，然后使用这个手机号去网站或平台注册，注册过程中产生的短信验证码，由卡商客户端上报给平台，经过接码平台的匹配之后，提取出验证码信息返回给用户。最后，用户凭借这条验证码，完成注册。



在短信验证码的对抗中，出现了很多新的形式。比如，整个注册过程中，可能需要接收多验证码，或要求用户向指定的号码发送一条验证码，也有很多平台选择了语音验证码。而接码平台，也在不断的改进，产生出了专门的发送验证码服务、语音验证码听码，还衍生出了另外一种网赚项目——“听码”。

项目ID	项目名称	匹配文本	类型	金额
2033	钱语音验证码【不能用于恶意刷单，仅供测试使用】	-	语音	2.00
2027	语音验证码【不能用于恶意刷单，仅供测试使用】	-	语音	2.00
2014	UC彩语音验证码【不能用于恶意刷单，仅供测试使用】	-	语音	2.00
2012	六合彩库语音验证码【不能用于恶意刷单，仅供测试使用】	-	语音	2.00
2003	性感可爱小闪闪语音验证码【不能用于恶意刷单，仅供测试使用】	-	语音	2.00
1999	式玩注册试玩奖励语音验证码【不能用于恶意刷单，仅供测试使用】	-	语音	2.00
1990	语音验证码【不能用于恶意刷单，仅供测试使用】	-	语音	2.00
1981	语音验证码【不能用于恶意刷单，仅供测试使用】	-	语音	2.00
1975	DSF语音验证码【不能用于恶意刷单，仅供测试使用】	-	语音	2.00
1974	彩票语音验证码【不能用于恶意刷单，仅供测试使用】	-	语音	2.00

3.2.3 打码平台

验证码（Captcha）是各个网站、APP常见的功能模块。

验证码（Captcha）全称是 Completely Automated Public Turing test to tell Computers and Humans Apart（全自动区分计算机和人类的图灵测试），是区分计算机和人类的一种程序算法。简单解释是一个答题的验证。系统向请求发起方提问，能正确回答的即是人类，反之则为机器。CAPTCHA 经过不断演化，已成为目前国内外各大互联网公司用于对抗网络黑产恶意行为（如恶意登录）的验证码安全策略，即我们现在俗称的验证码系统。

在网络黑产中，不法分子窃取网站数据库后，需要确认帐号对应的密码是否正确，将有价值的数据通过验证的方式筛选出来，这一过程黑话叫“晒密”，意即撞库。而“晒密”最核心的障碍就是互联网公司设置的验证码安全体系。每天面对数以亿计的“晒密”需求，黑产分子不可能人工逐个识别，而是需要提高“晒密”效率，批量识别。“打码平台”即是提供批量自动化识别各类验证码的专业服务平台。

2017 年 3 月，绍兴警方打掉了曾受很多羊毛党欢迎的“快啊”打码平台。这个平台通过运用人工智能机器深度学习技术训练机器，可以让机器如 ALPHAGO 一样自主操作识别，有效识别图片验证码，轻松绕过互联网公司设置的账户登录安全策略，给网络诈骗、“黑客”攻击等网络黑产提供犯罪工具。这是国内首个利用人工智能进行犯罪的案例。这也表明，当下风靡的人工智能技术，早已被用在黑产当中。

3.2.4 改机工具

改机工具，是通过劫持系统函数，来对设备信息进行篡改的技术手段。

Android 或 iOS 设备中，都提供了各种接口，用于获取设备的基本信息，比如设备标识符IMSI，IDFA/IDFV。而改机工具能够从系统层面劫持这些接口，当APP调用这些接口来获取设备的各项参数时，获取到的，都是改机工具伪造出来的数据。如果凭借设备参数来判断设备的唯一性，改机工具每次生成新的参数，就会被识别为一台新的设备。在特定的领域中，这种技术被大量使用。

Android hook

Android 的大部分改机工具都是基于 xposed 框架做的插件，需要 root。通过 HOOK 方式修改 IMEI, IMSI, 手机号，MAC地址，手机硬件信息，地理位置，安装包列表等。

iOS hook

iOS 的改机工具基于cydia框架做的插件，需要越狱。通过HOOK修改设备参数（包含序列号、UDID、IDFA、IDFV、IMEI、SSID、BSSID、SerialNum、地理位置）。一些高级的工具如nzt，还提供了多开和一键新机功能。

Android 模拟器

严格来说，模拟器并不算改机工具，但模拟器正在不断集成改机工具的一些功能，在风控领域中产生对抗。

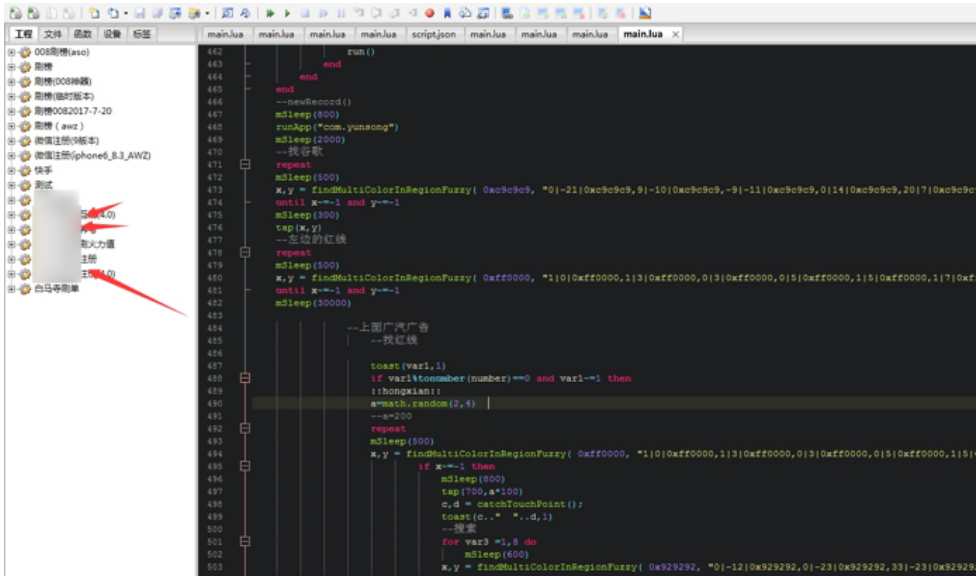
由于 hook 检测的对抗，黑产开始逐步转向自定制 ROM 的 Android 模拟器。这些模拟器具有一键新机的功能，每次启动所有的系统参数都会随机变化。这种模拟器并没有进行 hook 操作，也没有安装 hook 框架，所以比较难识别。

3.2.5 按键精灵

传统的按键精灵，想必大家并不陌生，按键精灵能够记录鼠标和键盘的动作，并进行重放，可以用来完成很多重复性的工作。深受大学生讨厌的英语视听说，就有人专门录制按键精灵的脚本，运行脚本后，就可以自动完成整套视听说的在线练习。（后来视听说为了对付按键精灵，故意把选择题顺序打乱，2010 年以后的大学生都没享受过这个待遇）。很多游戏代练，也会使用按键精灵，来实现自动打怪、自动采矿，甚至自动对话。

移动端的按键精灵，也是一样的，能够记录用户的触摸轨迹和输入操作。早期的按键精灵，通过录制用户的触摸轨迹来完成，发现到今天，大部分按键精灵，已经可以通过编写脚本来实现了。

以目前较为流行触控精灵为例，能够同时支持 iOS 和安卓设备，可以使用 lua 编写脚本，完成很多复杂的操作。

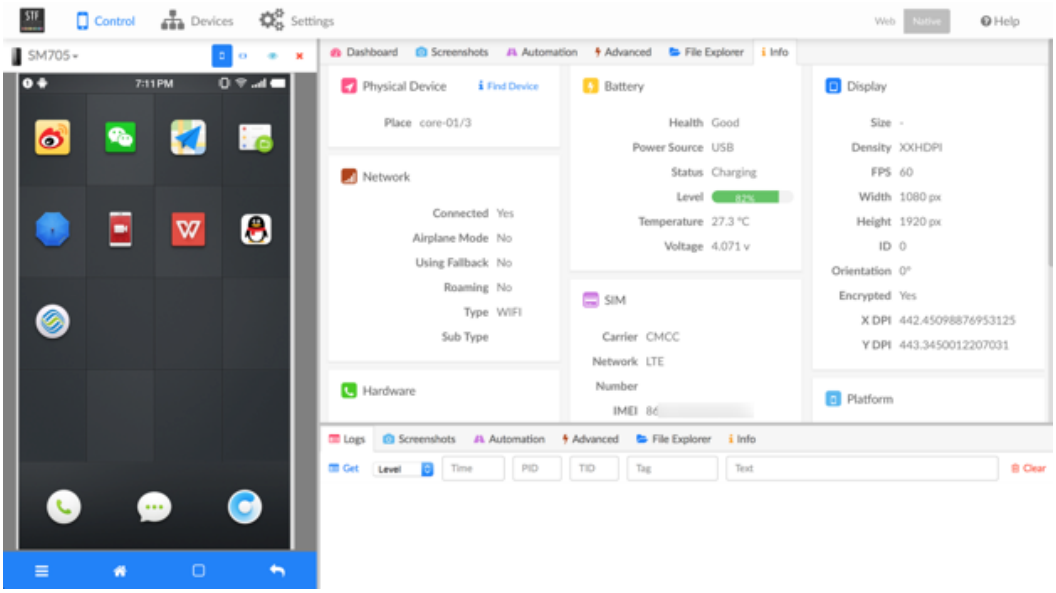


并且，配合特定的作弊工具，可以在适当的时候对设备进行备份或者清空，甚至生成全新的一套设备信息，以对抗设备维度的各种防控策略。

3.2.6 群控系统

群控系统，是模拟器作弊的升级手段。模拟器作弊和群控系统，都是为了打破越来越多的针对设备维度的限制技术而产生的。区别在于，群控系统都使用真机来完成。设备指纹技术的产生，让我们可以通过多种方式，来识别设备都否是模拟出来的。设备群控，应运而生。早期的设备指纹，仅仅以设备上的特定标识符，作为设备的唯一表示，包括：IMEI/MEID、IMSI、IDFV/IDFA等。随着模拟器的不断完善，逐渐产生了很多定制化的模拟器，可以随机生成上述的各项参数。

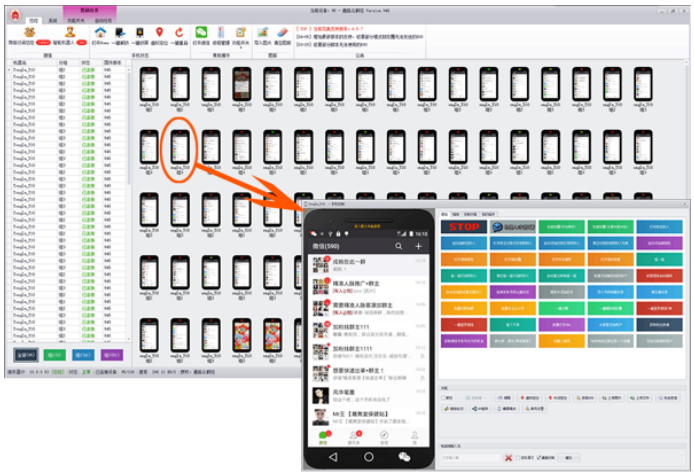
2015 年下半年，通过电脑来控制移动设备的技术产生，其中最有代表性的就是OpenSTF。



STF运行界面

2016 年下半年，群控系统首次出现在我们视野中，当时已经有小规模的团伙在使用群控系统。定制的低价安卓机，设备陈列架，加上群控系统和专用的工业级服务器，目前市场报价两万左右（30控），设备数量越多，价格也越高。

早期的群控系统功能，围绕微信营销展开，主要为微商服务。群控系统中，提供模拟定位、站街、摇一摇、批量导入通讯录等功能，来大量添加微信好友，再通过朋友圈发布、消息群发等功能进行定向的消息推送。某些群控中，加入了图灵机器人，可以和用户进行互动，产生真实的聊天记录。



通路云群控系统运行界面

此后，大批的互联网公司通过微信来发布各类营销活动，欺诈分子开始利用群控参加营销活动，赚取毛利。

同盾对市面上的安卓群控系统进行了较为深入的研究，这里做一些简单的介绍。安卓群控系统，都通过 adb 来实现对设备的控制。

adb 的基本功能如下表所示：

命令	说明
install path_to_apk	向安卓设备上安装一个应用
pull remote_path local_path	从安卓设备上下载一个文件
push local_path remote_path	向安卓设备上传一个文件
shell	打开一个交互UNIX shell，并执行命令
shell command	不打开UNIX shell，直接进行一个命令

此外，还有 Package Manager 和 Activity Manager 命令，提供了更多强大的控制功能，这里就不做一一介绍了。

比如，使用 adb 向安卓导入通讯录：

```
adb -s emulator-5554 shell am start -t "text/x-vcard" -d "file:///sdcard/contacts.vcf" \
-a android.intent.action.VIEW com.android.contacts
```

通过 Activity Manager，可以精确地控制安卓系统中的各种活动，比如打开应用、触发特定的活动或行为，甚至单独调用某一个类，来进行特定的操作。

各种开发语言中，都有 Android SDK 相关的库，可以在群控的基础上进行二次开发。比如，下面是某群控系统的一个微信自动打招呼插件（C#）：

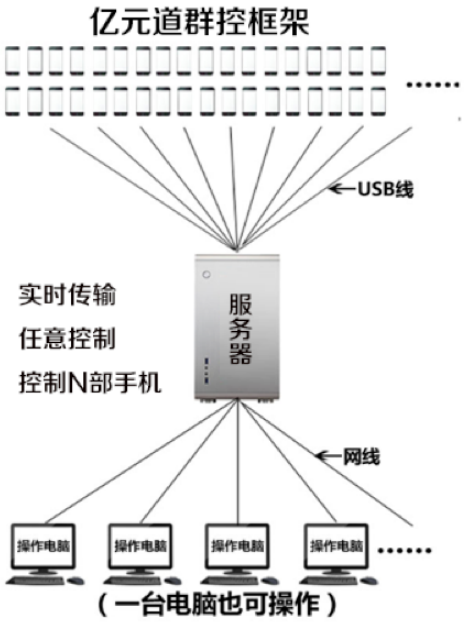
```
using System;
using System.Collections.Generic;
using System.Runtime.Serialization;
using System.Threading;
using System.Windows.Media;

namespace mysss
{
    public class Class1 : AndroidControlSDK.AndroidScript
    //继承AndroidControlSDK.AndroidScript来实现插件功能
    {
        public override string Name()
        {
            //返回插件的名称
            return "自动给附近的人打招呼";
        }
        //这个方法是插件的执行主体，所有功能都在这里执行
        public override void RunScript()
        {
            //显示调试日志，正式用时可以不开启这个
            ShowLogConsole();
            //在手机屏幕上显示运行状态
            ShowStatus("正在打开附近的人..", Color.FromRgb(78, 17, 255));
            //打开附近的人界面，这个具体参数请查看开发博客
            var dic = new Dictionary<string, string> { { "act", "opennearui" } };
            SendIntent(dic);
            //冷却1000毫秒
            Thread.Sleep(5000);
            //定义个int变量用于计数
            var count = 0;
            //定义一个变量为打招呼的内容
            var zhaohu = "hi，你好啊";
            //在手机屏幕上显示运行状态
            ShowStatus("正在获取附近的人“列表”..");
            //获取所有的昵称 com.tencent.mm:id/agg
            //这个是附近的人列表里的昵称资源id，这个可以通过uiautomatorviewer.bat来获取
            var nicks = GetUiTexts("com.tencent.mm:id/agg");
            Console.WriteLine("获取到的昵称数量：" + nicks.Count);
            //循环给所有昵称打招呼
            for (var index = 0; index < nicks.Count; index++)
            {
                var nickname = nicks[index];
                ShowStatus("正在加“" + nickname + "”[累计：" + count + "]..");
                //查看是否包含这个昵称
                if (FindObj(nickname).Contains("成功找到元素"))
                {
                    //包含就点击它
                    if (FindAndCLickObj(nickname).Contains("true"))
                    {
                        //冷却1000毫秒
                        Thread.Sleep(1000);
                        //查找并点击“打招呼”
                        var result = FindAndCLickObjByRegex("打招呼");
```

```
                    var result = FindAndCLickObjByRegex("打招呼");
                    //输出结果到日志
                    Console.WriteLine(result);
                    //如果点击成功
                    if (result.Contains("true"))
                    {
                        Thread.Sleep(1000);
                        //查找输入框输入内容
                        FindAndInutText("android.widget.EditText", zhaohu, 0);
                        Thread.Sleep(2000);
                        //添加好友
                        FindAndCLickObjByRegex("(加为朋友|发送)");
                        Thread.Sleep(1000);
                        //返回
                        FindAndCLickObj("返回");
                        Thread.Sleep(1000);
                    }
                    else
                    {
                        //如果没有打招呼按钮则直接返回（一般是已经添加过了）
                        FindAndCLickObj("返回");
                    }
                }
            }
            //计数器加1
            count++;
        }
    }
}
```

群控系统的插件开发，很大程度上受制于群控系统本身的功能，和开发人员的技术水平。但绝大部分使用群控系统的人，其实并不具备开发能力，仅仅是单纯地使用群控系统进行营销。

目前市面上流行的群控系统一般架构如下：



adb 可以同时连接多台安卓设备，理论上，可以通过一台 PC 对多台安卓设备进行批量控制。但是，由于硬件问题，一般的 PC 机主板，最多承载 36 个 USB 设备(某些只有 16 个或 32 个)，限制了群控系统能够连接的最大设备数量。所以一般会使用专用的服务器，配备工业级主板。

adb 在服务器上运行，提供向设备下发命令的功能，控制机（分为主控机和分控机）在客户端上进行操作，所有操作信息通过 API 发送给服务器，由调试服务器转化成 adb 命令，下发到所有设备上执行。

```
// XiakeAdbWeb.Default
public static string Cmd(string cmd, string arg)
{
    string result;
    try
    {
        Process process = new Process
        {
            StartInfo =
            {
                FileName = "sudo",
                Arguments = cmd + " " + arg,
                UseShellExecute = false,
                RedirectStandardInput = true,
                RedirectStandardOutput = true,
                RedirectStandardError = true,
                CreateNoWindow = true
            }
        };
        process.Start();
        result = process.StandardOutput.ReadToEnd() + process.StandardError.ReadToEnd();
    }
    catch (Exception arg_8E_0)
    {
        result = arg_8E_0.Message;
    }
    return result;
}
```

上图是对某群控系统服务端程序逆向之后得到的代码片段。

群控系统的运行，主要依赖于 adb，即便设备没有 Root，也是可以用于群控的。但市面上所有的群控系统，都要求所有设备先使用特定的 ROM 刷机，然后 Root，再安装 Xposed 框架及其他的必备工具。

> 关于 Xposed 框架 Xposed 提供了一种在不修改 APP 的情况下，直接在内存中，修改 APP 数据的可能。这个数据修改包括两方面，一方面是 APP 通过 Android 接口获取的各种系统参数，包括定位信息、IMEI/IMSI 等另一方面，APP 本身的各种数据，也可以被修改，比如微信的红包、已被撤回的消息、内置的各种广告信息等等。

实际上，基于 Xposed 框架可以做很多很多事情，目前在群控系统中的应用还比较少，使用最多的，是 X 输入法，用户进行各种文字输入。比如，下面的插件是针对天猫和淘宝的，通过 Xposed 来监控 APP 中的各种优惠活动，自动领取优惠券或红包，如果群控系统使用类似的插件批量抓取红包，效果会非常明显。

某些群控系统还集成了图灵接口，能够进行与人进行常规的对话，这大大增加机器行为识别的难度。

当群控系统、改机工具和移动端按键精灵结合到一起的时候，对平台来说，就是灾难性的。每台设备上都部署了相应的工具，只要录制好操作脚本，下发到所有设备上重复执行，配合前面提到的接码平台，能够大幅提升薅羊毛的效率和通过率，如果没有靠谱的设备指纹技术，仅通过设备上的部分字段来进行防控，对目前群控的手段来说，几乎起不到任何防控作用。

3.2.7 开发者

开发者在整个黑色产业链中，扮演者非常重要的角色。数量众多的开发者，不断地在给整个黑产军团提供大量的自动化工具、作弊工具、脚本、插件，大大提升了黑产的作业效率。

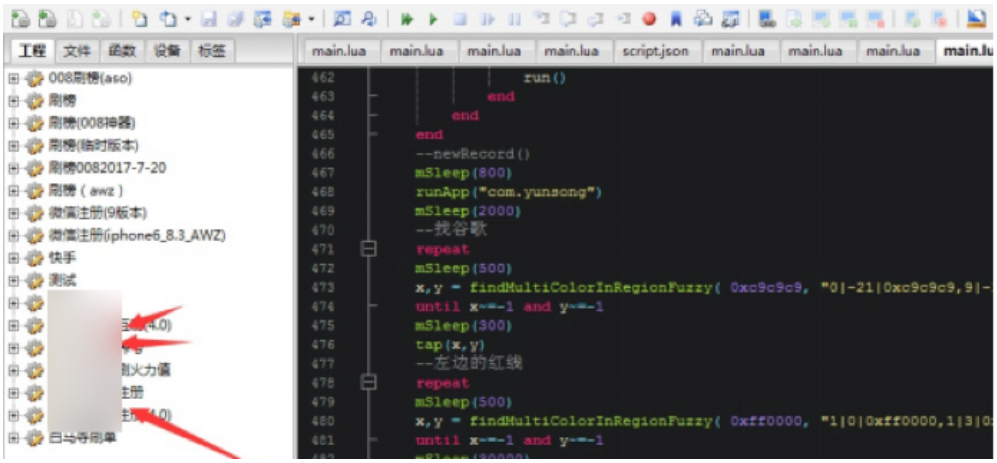
工具开发

琳琅满目的黑产工具，几乎是黑产的必备手段。注册机、改机工具、群控系统，这些工具越来越完善，呈现出一体化、定制化的趋势。一般的，注册机和改机工具的开发，大多以工作室的形式进行。相比之下，群控系统拥有更大的市场，能够提供定制化的开发，有完善的售后服务，即使完全不具备技术能力的人，也能够正常使用这些工具。

插件/脚本

尽管大部分的作弊工具，都可以傻瓜式的操作，不要求使用者具备相应的技术水平。但这些工具的设计，是为了满足通用性的作弊，针对特定的应用场景、或平台有更加复杂的审核机制，就需要在作弊工具的基础上进行改造，或者使用特定的插件来完成。

比如前面介绍触控精灵，其中的截图来自于一个专攻某视频平台的黑产工作室。



其中就有专门用于养号的脚本，会自动下载其他播主的视频，对视频文件进行简单的编辑之后，再上传到垃圾账号的主页上去，过程中或使用一些技术手段，来规避平台对视频文件的校验，具有非常高的针对性。

类似的，Xposed 插件、群控插件、按键精灵脚本等等，都有非常丰富的插件资源可以使用，也有很多专门的开发者群，来接受各种的定制化需求。

软件破解

软件破解，无疑是众多开发者中技术水平最高的一群人。他们往往具备较高的逆向能力，能够破解 APP 中复杂的加密逻辑，进而针对性地编写脚本或工具来完成特定的验证或审核流程。或者逆向出 APP 内的验证逻辑，再交由具备开发能力的开发者去制作专门的工具。

临近“双11”，各大电商平台都在进行各项准备，黑产也没有闲着。在黑产聚集的论坛中，针对各大电商平台的破解、逆向订单数量，都有明显的上升趋势。

除上述的几类开发者，还有一些较为分散的技术人群，为接码平台、打码平台提供着一些琐碎的技术支持，并从中获得一定的提成，相比之下，这类开发者对整个黑色产业链起到的作用要小得多。

第四章 以 QQ 群为主的羊毛党调查

近几年 QQ 和微信风靡全国，QQ 号或微信号人手一个甚至好几个。这两种沟通方式与人们的日常生活、学习、工作都密切相关，不少羊毛党也借势在这些平台大势发展。早期网赚群体中的小部分人，建立了博客、工作室，组建起具有一定规模的 QQ 群，为羊毛党提供活动线报、经验，同时也积累了大量的下线。如今，QQ 群已经成了他们活动的大本营。

记者以“FD”和“薅羊毛”为关键词，加了一些 QQ 群进行调查，对集中在 QQ 群中的薅羊毛产业链有了一定发现。说起“FD”，薅羊毛圈内人士应该不陌生，这个词最初是指一个名为 Fiddler 的抓包工具。由于不少羊毛党薅羊毛时会用到抓包工具，因此就衍生出一些以“FD”为关键词的薅羊毛 QQ 群。

刚加入时，发现好几个群都没有什么特殊内容，而且全员禁言。只有几个管理员不断发消息，表明：此群没有有效信息，并发了新群的链接。

记者加入某个新群之后，发现立刻被管理员移出了第一次加的群。这个新群是该集团下的第 6 个群，前五个群 2000 人都加满了，第六个群仅创建了 20 天就已经有 1700 多人，而且还不断有新人加进来，每天在线的成员平均有 1200 多人。两天之后，这个群也已经加满，群主再一次开了新群。

中转群

群介绍和群公告里，群主都要求成员多拉人进群领福利

由于群主禁止重复加群，也就是说，仅这一个集团就有上万人的规模，按照 2/3 的比例，这个集团每天基本有 8000 多人在线，一看到线报就立刻去哄抢。

4.1 薅羊毛QQ 群群主

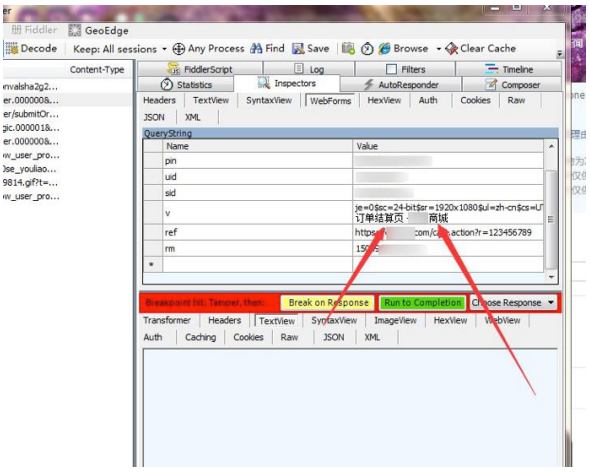
新的一天，程序员小 A 醒来之后，习惯性地打开手机看看自己所在的十几个群，有些群的消息是 99+，有一些只有十几条。“估计群主该拉人了”，他心想。果然，过了一会儿，两个不太活跃的群分别都发了红包，伴随着红包的还有一句话：拉人进群领红包。其中一个群主，则直接把群昵称改成了这句话。

小 A 在家乡就业，是当地一个小公司的开发人员。在研究工作的时候无意间发现某个电商平台有漏洞，而利用这个漏洞可以免费购买商品。有了这次发现，他便有意无意在网上搜索相关消息，并下载了一个 fd 工具，结合查到的信息和自己的技术，经过一段时间研究之后，他成功以低价买到了正价商品。此后便一发而不可收拾。

在这十几个群里，小 A 主要担任技术人员的角色，他不断改进一些抓包、改价工具，有空就会尝试挖洞。这些工具和漏洞可以卖给羊头，再由羊头分发给自己管理的群成员。此外，如果群里有人问问题，他有空会回复几句，很轻易就能与新手私聊，向对方介绍工具，如果对方表示感兴趣想再进一步询问，就需要拜师交学费。小 A 一共有近 60 个徒弟，平均学费 288 元，仅拜师费这一项就为他创收 1.5 万左右，而每个徒弟出师之后（成功实施一次改价购物），还会拿出一些红包孝敬师父。小 A 说，平时工作忙，懒散一点每个月也能保证一千多元的收入，就当闹着玩了。此外，自己还有几张黑卡，可以制造假身份接收改价购物而不被查到。偶尔还可以糊弄那些新手徒弟，以一百到几百不等的价格把同一个假信息多卖几次。

> 有的比较精，不给钱。有的没见过世面，不懂其中的门道，所以我一说就愿意给钱。对于这种人，我还能拿到他们的微信号、支付宝或者 QQ 号，伪造新的身份去撸其他商品。我是他们师父，我一说他们基本都听，跟他们要号也不会亏待他们，偶尔撸到手机等好东西，也会直接送给他们。

小 A 称自己已经基本免费撸到了十几部手机，安卓苹果的都有。有的自己用，有的拿去卖钱了，有的送徒弟了。站到这个 QQ 群产业链的第一层后，他似乎变得大方了一些，也看开了一些。他不再花很多时间亲自去撸 FD，一来费时间，二来也不想再多冒险。毕竟拜师费和一个软件多次转卖，就能轻轻松松获得收入。又何必给自己找太多麻烦呢。



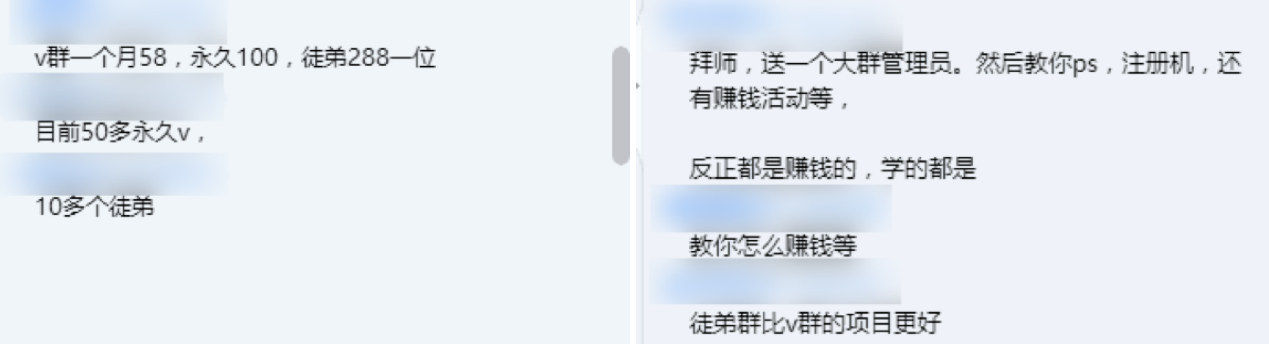
FD 改价

而另一个群主小 B 的身份则更加复杂。小 B 是某高校计算机系的大二学生，也是偶然接触到黑客知识，最后加了很多薅羊毛活动群。不过，跟小 A 比起来，小 B 成为群主的路，多了一些曲折。

> 我去年才接触到这一块。最开始也是什么都不知道，看到有人收徒就去拜师。2888、1888、288、188（元），各种层次的学费都交过。每个师父教的大同小异。最后学得多了，就自己总结出一套理论和实践，也收了一些徒弟，慢慢建立起自己的群和圈子。虽然学费贵，不过慢慢也能赚回来。现在我平均每个月能收入五千，生活费不用愁了。这个圈子的发展大概都是这样，师父带徒弟，徒弟出师了再去收徒弟。所以这里有很多群，但凡大一点的群主，要么是自己技术很好；要么是自己认识的人多，可以拉很多人；要么就是拜过师。

小 B 自己收了十几个徒弟，开了三个 QQ 群。一个群是散群，平时发一些秒杀活动，群成员大多是通过发红包或者熟人拉进来的。第二个群是 VIP 群，大多是从散群里引流过来的。散群里只要有人表现出进一步询问或学习的意向，他就会去回答并介绍自己的业务：交 58 元可以进 VIP 群一个月；交 100 元可以永久进入 VIP 群；交 288 元可以拜师学艺。据小 B 称，VIP 群的线报比大群的线报更及时也更优质，进群可以很快回本。徒弟群里则集中了徒弟、同学、亲友，方便平时教学、开车（有活动时亲自带着徒弟亲友一起薅）。此外，他自己也加了三五个其他类似的群，作为普通成员搜集线报，再发到自己的群里。

小 B 说，自己平时很忙，一方面要认真学习专业知识，一方面又要钻研各种软件，管理自己的群。“我不觉得这些违法，都是凭自己的技术赚来的。平时忙但也很充实，挺好的。”



VIP 群和收徒流程

黑客工具

除了小 A 和小 B 这种自己卖技术带徒弟的群主，薅羊毛 QQ 群里还有另外一类群主，被称作羊头或代理。大一些的羊头基本都有十几个群，平时靠小额多人的红包或一些鸡汤口号维护着群里的活跃度。他们一般会跟 P2P 网贷平台合作，新的平台有拉新活动，或是老平台的新活动需要流量时，一般都会找到代理和羊头，给回扣请羊头推广。而代理或羊头则拿着平台给的注册链接，发放到自己管理的各个群里，群成员只要从这个链接进入平台注册或投资，就能拿到返现。而羊头只需要收取人头费。以某平台投资返现为例，平台给到羊头投资 1000 一个月返现 55 的项目，羊头有 10 个群，一个群 1000 人，也就是能拿到 10000 人的单子。羊头给群成员的返利是 50，那么羊头自己就能抽到 5 万元的回扣。只要平台靠谱，不卷款逃跑，这个项目就能让羊头和群成员都赚到利润。如果这个单子分散到 100 个群，按一个群 1000 人算，那么企业的五、六百万的推广预算就全部被薅走了。

代理和羊头的盈利模式

此外，这些羊头也会跟小 A 这类技术型黑客合作，看到刚上线的新平台有了拉新活动（例如注册送体验金等），就会找小 A 他们去挖漏洞进行破解。一旦找到破解方法，就会在群里售卖或发布给群成员，分分钟就能让平台亏得血本无归。

某位知情人士告诉记者，有一次群主发布了某大型金融公司某个返现活动的漏洞，注册时反复上传相同身份证都会默认为新用户。2 天之内，就有十几万人利用这个漏洞反复获取大量返现。所幸该公司作为大平台风控较为及时，很快就修复了漏洞，但还是造成了不小的损失。

4.2 薅羊毛 QQ 群成员

作为薅羊毛 QQ 群的主力，普通群成员构成了庞大真人 DDoS 阵营，只要看到了活动，只要有空，就会去薅一把。他们信奉的宗旨是“勿以毛小而不薅，勿以毛大而舍命薅”。哪怕每次活动的利润很小，但毕竟只是动动手指的事情，何乐而不为呢？

利用商家平台漏洞

记者在调查过程中共加入几十个 QQ 群，每天每个 QQ 群的消息都有几百条，就算是禁言群，机器人管理员也能发出上百条秒杀、返利、领红包等各种活动信息。小到某游戏平台注册抢 Q 币，大到聚划算上手机或者电器的优惠券抢购或秒杀，各种信息层出不穷。归纳下来，有微信公众号的活动红包；有中国移动、中国联通、中国电信乃至支付宝等推出的流量优惠活动；有辣条、老干妈、面包等零食的抢购；有纸巾、洗衣液、衣服、鞋子等日用品的秒杀；还有腾讯等各大视频网站 VIP 会员；下载 APP 领代金券或红包提现；以及邀请注册、投资返现等等。他们时刻关注着群里的动态，一有新消息，便倾巢而出，如蝗虫过境般将活动平台一扫而空。

举例来说，某天上午，有一个二十几块抢价值几百块的月饼礼盒活动，仅半小时左右，群主就进来宣布 50 万库存已经被抢光。

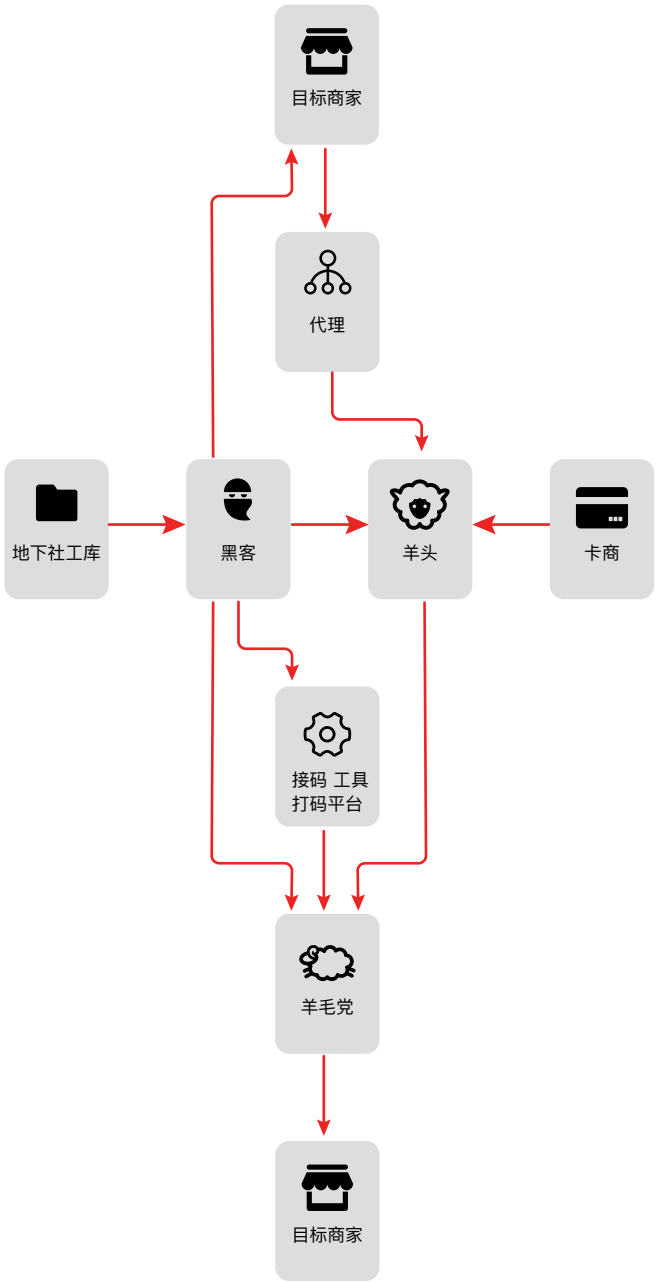
月饼礼盒活动

这种薅羊毛群可以按照薅的对象分为三大类：一类以网贷理财、广告推广为主；一类以抢实物、话费、流量、红包等为主；还有一类以FD 改价、改数据抢手机为主。由于类别不同、要求不同，群成员的身份也不太相同。网贷理财类QQ 群的成员大多有稳定收入（工资或者生活费），有闲钱可以投资；第二类人员复杂，管理员大多是职业羊头或有正式工作，而成员则包括学生（不少是大中专学生，也有很多未成年的学生）、待业在家的社会人士等；第三类人大多有一定技术背景，要么是 IT 相关专业的学生，要么在从事 IT 相关的工作。这三类群中，第一类第二类群的比例较高。

一个在某薅羊毛 QQ 群里待了两年多的用户告诉记者，群里大部分都是学生。群主平时会督促群成员去各大贴吧打广告拉人，也会在群里发红包，让群成员拉亲朋好友入群。

4.3 基于 QQ 群的薅羊毛产业链

根据薅羊毛 QQ 群的群主和群成员成分调查与分析，可以推断出一条以 QQ 群为主的薅羊毛产业链：

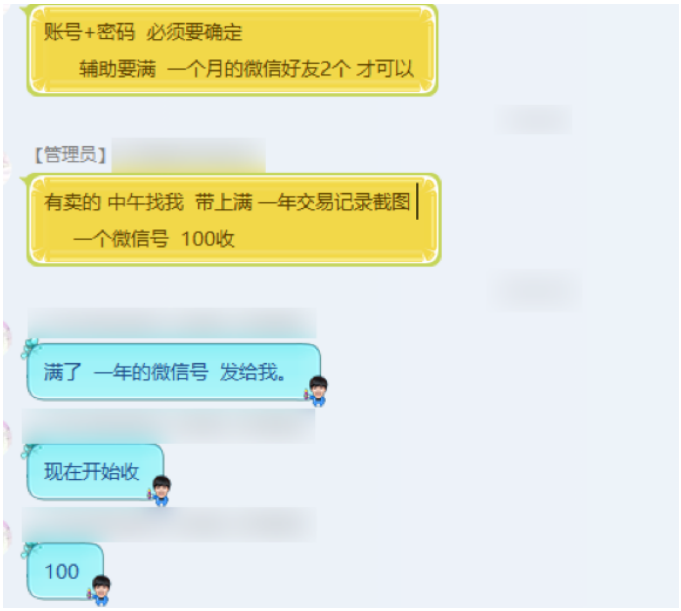


4.3.1 黑客

去各大平台挖洞；开发制作各种软件，如自动注册机、自动刷单器、 FD 抓包工具、换 IP 工具等；通过社工或撞库，获取黑卡资料、身份信息等；同时与代理或者广告商（团伙工作室）合作，维护接码、打码平台或者代理的公司网站（很可能这些网站背后的主要运营者就只有几个人）；

代理 IP

工具及身份信息



微信号买卖

4.3.2 代理

与网贷平台或者某些软件开发公司合作，接单、推广、打广告；有一些做了简单的网页，成立工作室，自称广告公司；据知情人士表示，这些平台大多是骗子平台；此外，还有一些推广软件的平台利用色情等信息吸引下载，提高软件下载量和排名；

代理平台

利用色情信息骗取下载量

4.3.3 羊头

从代理处接单，从黑客处获取工具、漏洞，从各个群获取线报；成立并管理 QQ 群，拉人头；

4.3.4 卡商

提供大量手机卡用于身份验证。据记者调查，近一年来，大量来自缅甸、越南等东南亚国家的手机卡开始进入国内手机黑卡产业。这些卡支持 GSM 网络，进入国内后可以直接使用，无需实名认证，而且可开通微信等服务。同时，这些手机卡基本是 0 月租，收短信免费，成本低，非常适合手机黑卡产业使用，且使用比例越来越高。

4.3.5 羊毛党

有一些利用业余时间赚外快；有一些没有正式工作，或者身处偏远地区，靠整天刷单或秒杀活动而获取利益。

4.3.6 常见工具

手机安卓模拟器、信息修改软件或插件（FD 软件等）、接码平台、VPN （IP 代理服务器）、自动注册机、自动刷单机；

4.3.7 常见活动

手机安卓模拟器、信息修改软件或插件（ FD 软件等）、接码平台、VPN （IP 代理服务器 ）、自动注册机、自动刷单机；

1

关注微信号参与抽奖等活动：关注微信公众号，回复关键字或直接点链接参与活动，抽红包或实物奖励；

2

娱乐、游戏：集中于 QQ 或微信游戏，或者利用 QQ 号或微信号注册各大视频直播网站等；游戏或账号达到一定等级后领取红包或抽 Q 币，还可以卖账号；互联网发展趋势

3

打鱼和斗地主：这是两种特殊的游戏，带有推广性质；注册并赢得虚拟币到一定金额就可以获得返现；存在银商倒卖现象；

4

微盘：类似于股票，买涨买跌。一般为注册送券，一次交易后收益可以提现；

5

理财（最经典的薅羊毛活动）：一般为注册送体验金；有的可以直接提现，有的需要投资后提现；此时，利用身份证、手机号等信息以及卡商、接码平台等手段，就能提取大量资金，牟取暴利；

6

搬砖：通俗来说就是拉人头；自己在平台注册之后，再邀请好友获得人头费，拉够一定的量就可以提现；

7

人头项目：跟搬砖差不多；不过这类人头项目大多集中于理财投资类平台，需要绑定身份证、银行卡等信息，所以大多需要真人，难以利用接码平台；

8

博彩：大多为网址，也有一些是软件。这些人一般不充钱，利用注册送的彩金进行活动；几个人组队对押，或者使用改价软件修改倍率，总能获利；

9

官方活动接单：优酷等视频 APP 送会员、电信运营商送流量，或某些新软件推广活动，可以去接单；接单后，利用生成的初始链接邀请客户，根据数量获得虚拟商品或现金奖励；

10

代抢手机：利用 FD 等改信息工具或自动化工具，在个手机厂商新品发售时抢购手机，转手倒卖赚差价。

微信群的模式与 QQ 群类似。其缺点在于不便保存文件，优点在于更便于分享内容，且更有利于微信公众号活动和微商的传播。此外，以薅羊毛为关键词，也能在微信中搜到很多相关的公众号。

在调查中，我们还发现，初创的 P2P 平台、有 KPI 压力的运营人员或乙方、融资平台、代理商、小品牌以及一些软件开发商等，为了流量和人气，不惜搞各种活动，甚至直接找到所谓的媒体、推广公司（团伙工作室），拿出钱给代理、羊头回扣，通过羊头拉人给平台打广告，为自己博得关注，或者做出一些虚高的数据。

此外，羊毛党也会遇到被反薅的情况。据知情人士透露，这些 QQ 群和微信群中涉及的网贷平台中， 80% 以上都是骗子平台，在骗取羊毛党投资之后，就卷款而逃。而被骗的羊毛党，也无法声张，只能自吞苦果。

第五章 羊毛群体分析

5.1羊毛团伙

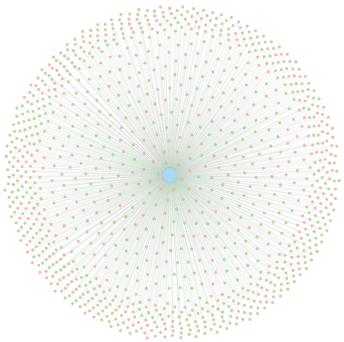
根据同盾科技反欺诈研究院对羊毛的分析，羊毛党主要分为两种：散户和羊毛团伙。

散户的羊毛党，由于资源有限，能够持有的手机号、身份信息和设备都非常有限，对平台造成的损失，并不是很大。
而相比之下，羊毛团伙有用大量的资源，并且能够借助各种工具，实现自动化的薅羊毛。对平台而言，这类羊毛党，是首要的威胁。

对羊毛团伙的识别，可以通过知识图谱来进行。一般在薅羊毛过程中需要使用大量账号，但是羊毛党所使用的设备是固定的，一定时间内不会发生变化。那么，通过知识图谱来建立设备与手机号的关联关系，就能够发现某些设备上，曾经使用过多个手机号进行注册，或者某个手机号在多个不同的设备上用于注册。这样的关联关系，我们定义为“欺诈团伙”。

对2017年前三个季度的羊毛党数据进行关联分析，我们总共发现了约110万个“欺诈团伙”，超过400万个手机号被这些团伙用于薅羊毛。

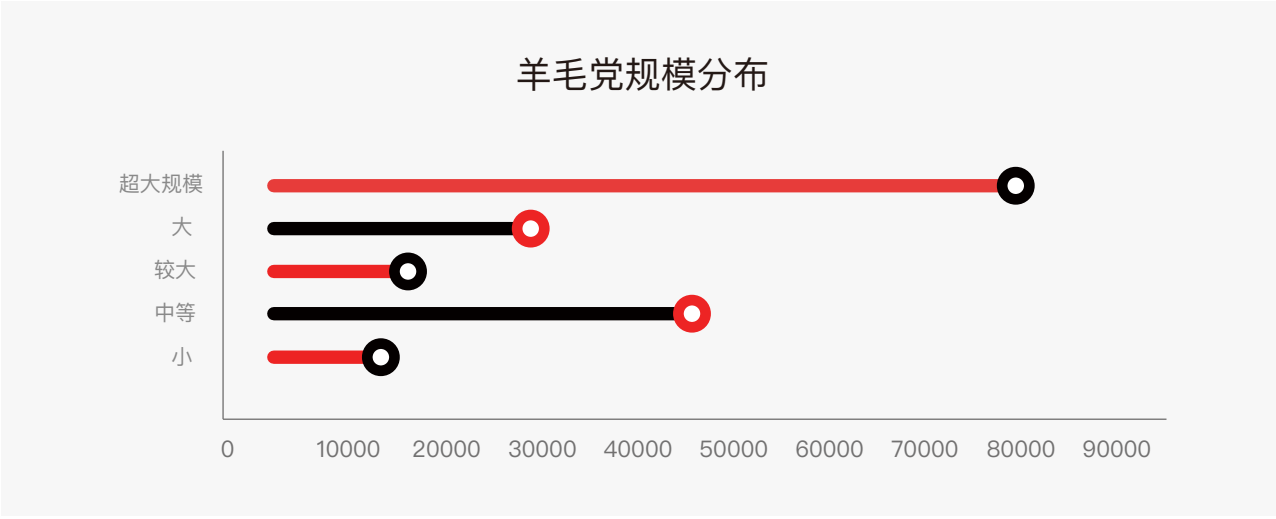
其中的一个典型的团伙结构如下:



上图中，位于中心的是羊毛党所使用的一台 iOS 设备，
与之关联的是 1000 多个被用于薅羊毛的手机号

根据监测，2017 年出现的羊毛团伙中，最大的团伙持有上千台设备，累计经手的手机号数量达到 250 万之多。假设一个手机号在一次活动中能够获利 20 元，那么仅这一个团伙在 2017 年前三季度的毛利大约有 5 千万左右，而他们的成本在 5 千万面前则不足一提。 这种怪兽级别的团伙，在技术能力、经济实力方面都不容小觑，对平台的危害甚大。

下图是 2017 年监控发现的所有羊毛团伙在规模上的分布。



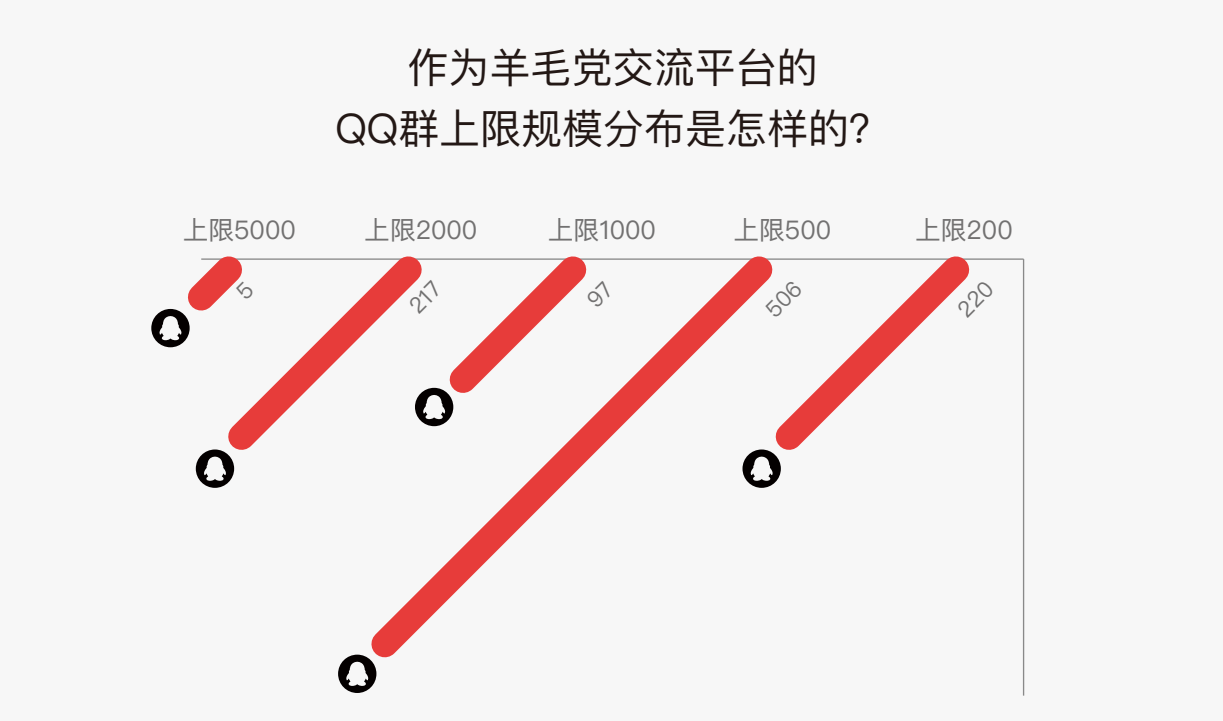
监控数据显示，这种超大规模的羊毛党团伙数量就已经超过 8 万。由此可预估，整个薅羊毛产业链对企业造成的损失已经达到千亿级别。

5.2 FD 群与薅羊毛群数据分析

我们调查了大量 QQ 群组，对群成员分布情况进行了统计。
统计到的 QQ 群组总数超过 1000 个，其中最大的群组人数为 4460 人，平均每个群组人数约为 505 人。

5.2.1 群上限分布

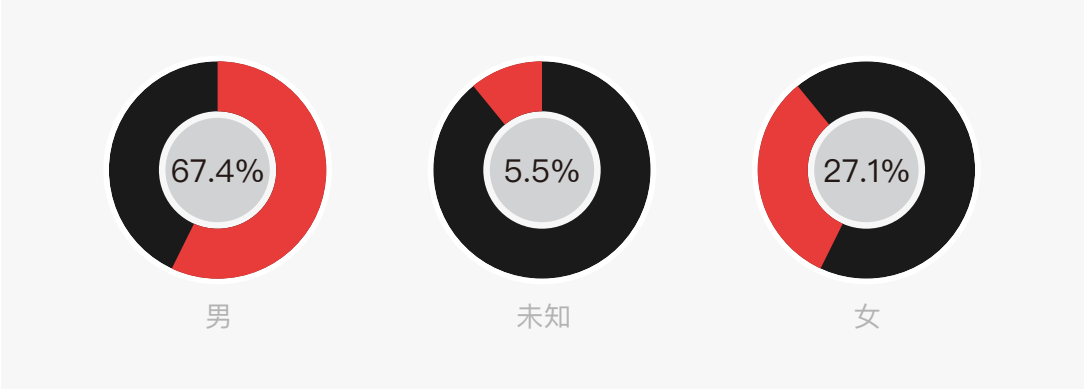
我们调查了大量 QQ 群组，对群成员分布情况进行了统计。
统计到的 QQ 群组总数超过 1000 个，其中最大的群组人数为 4460 人，平均每个群组人数约为 505 人。



QQ 群上限能够反映一个 QQ 群的容量信息，对于了解群成员也提供了重要线索，统计发现，群上限 200 的群组有 220 个，上限 500 人的群组有 506 个；上限 1000 的群组有 97 个；上限 2000 的群组有 217 个；上限 5000 的群组达到 3 个。

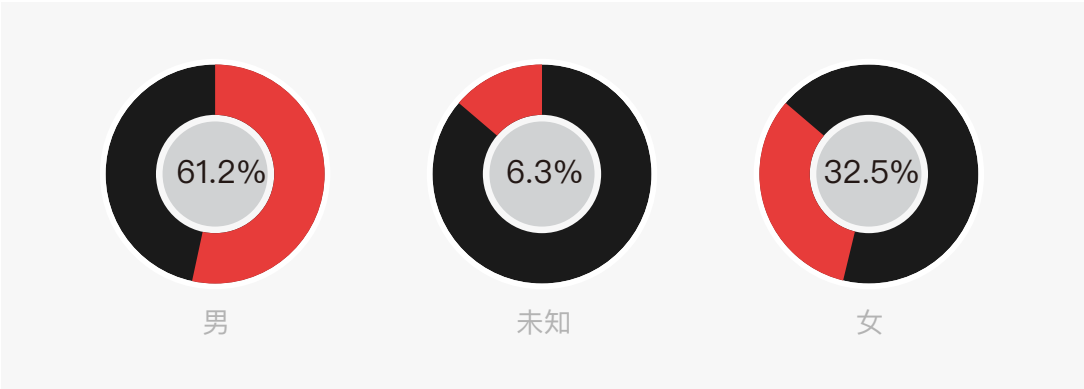
5.2.2 男女比例

我们调查了大量 QQ 群组，对群成员分布情况进行了统计。
统计到的 QQ 群组总数超过 1000 个，其中最大的群组人数为 4460 人，平均每个群组人数约为 505 人。

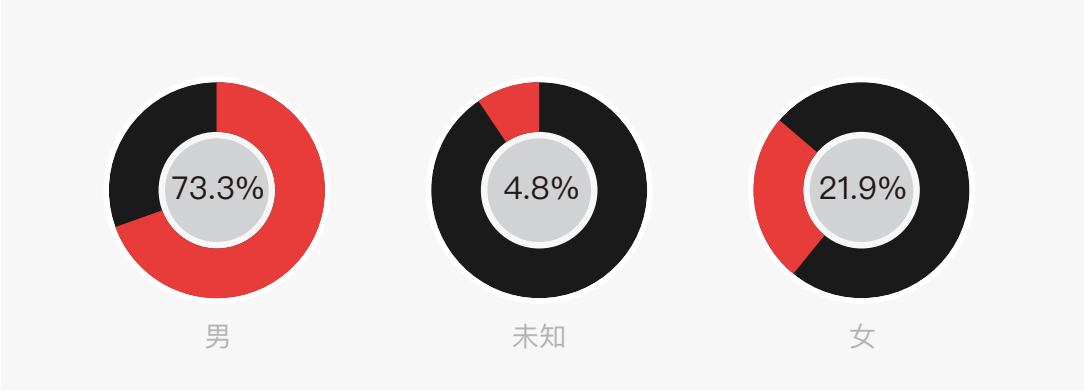


男女比例

根据 CNNIC 今年发布的《第 40 次中国互联网络发展状况统计报告》，截至 2017 年 6 月，中国网民男女比例为 52.4:47.6，同期全国人口男女比例为 51.2:48.8，网民性别结构趋向均衡，且与人口性别比例基本一致。[1] 而在薅羊毛相关领域，男女比例特征突出：在调查的 QQ 群总体样本中，男女占比分别为 67.4% 和 27.1%。其中，在调查的投资类 QQ 群样本中，61.2% 的群成员为男性，女性成员为 32.5% （另有 6.3% 未登记性别）；实物、红包群中，男性占比达到 73.3%，女性为 21.9%，未知性别为 4.8%。

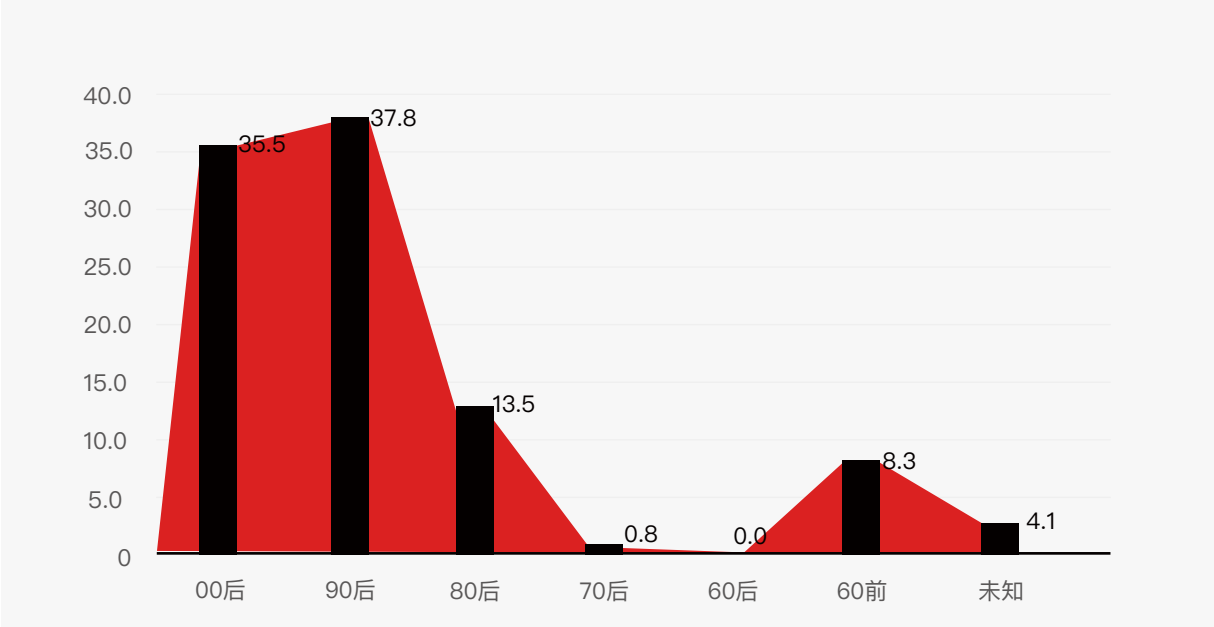


投资类QQ成员男女分布（%）

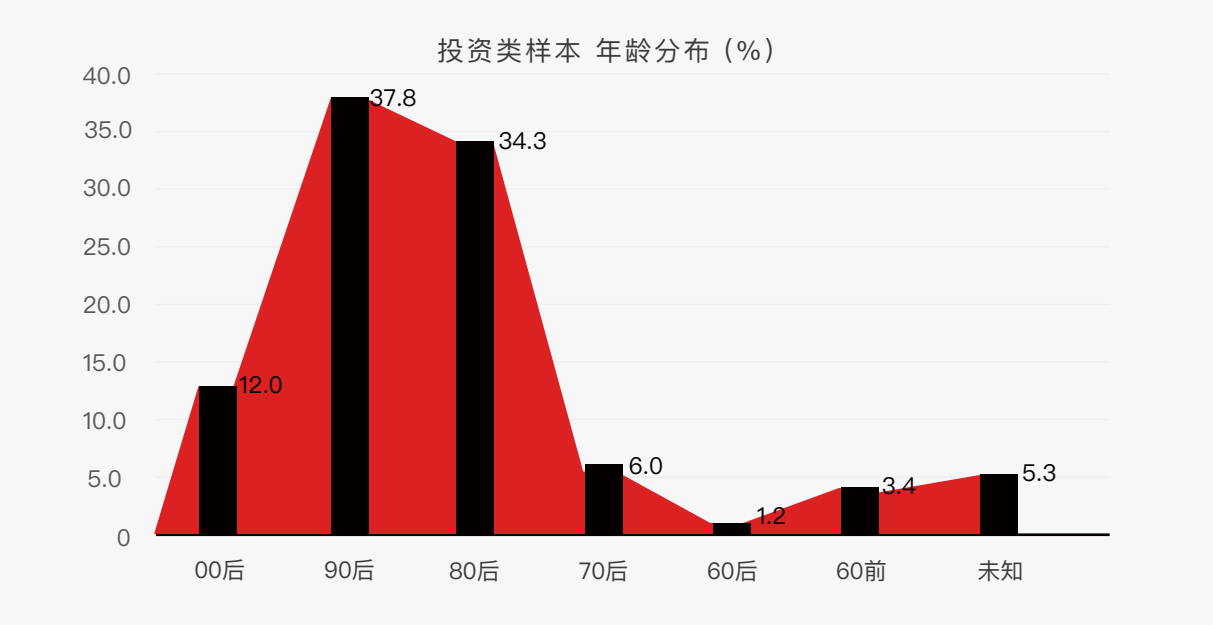


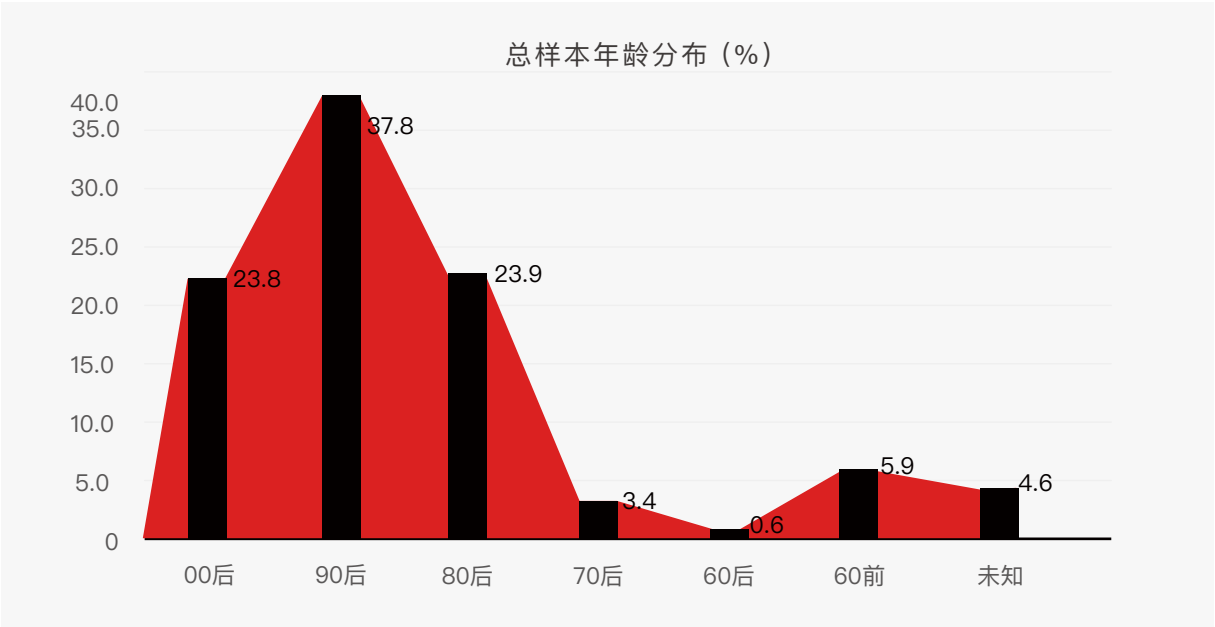
实物、红包类QQ群成员男女分布（%）

5.2.3 年龄层次



总样本年龄分布（%）



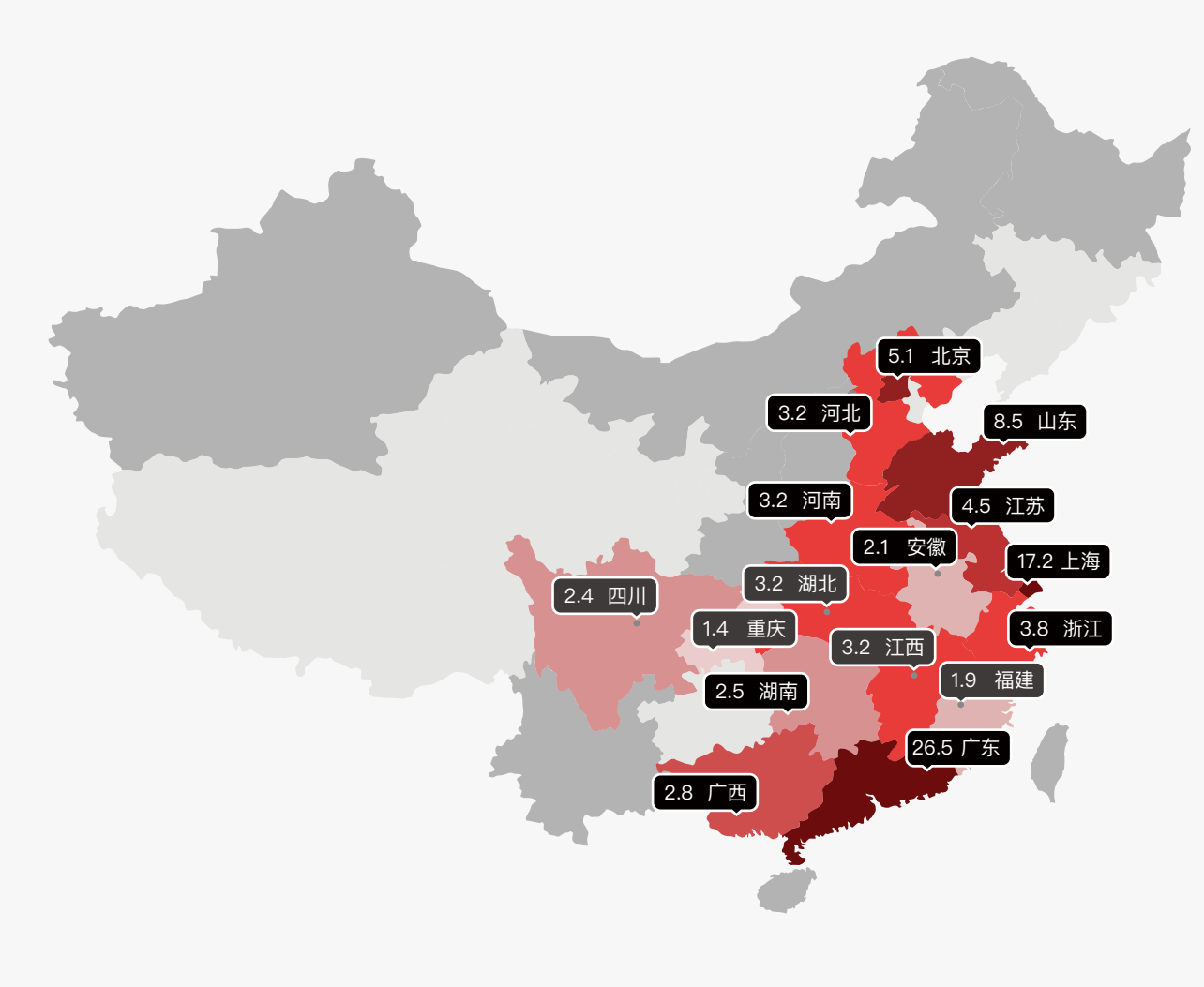


在年龄分布上，两类样本呈现出不同的年龄特征。投资类样本中，90 后（18–28岁）与 80后（28–38岁）人群占比都在 30% 以上，分别为 37.8% 和 34.3%，00 后占比为 12%，其他年龄段的人群都在 6% 以下。而在实物、红包类样本中，00 后（8–18岁）与 90 后（18–28岁）的占比达到 35% 以上（分别为 35.5% 和 37.8%），相比之下 80 后的占比为 13.5%，而总样本中，90 后所占比例最高。

5.2.4 地域分布

由于 QQ 没有提供群成员在全国的完整的分布情况，并且不同 QQ 群组的成员分布参差不齐，我们可以通过以下两种方式了解成员地域分布。

首先是 QQ 群中的成员统计。通过调查我们发现，群组成员分布的地区主要存在于广东、北京、山东、河南、苏州、江苏、浙江、上海、重庆等。其中出现频次较高的省份是广东、北京、山东、河南，在群成员中的占比分别为 6.36%、5.51%、5.32%、4.81%。



群地域分布（%）

除此之外，我们还统计了 QQ 群地点，这是出现在群资料中的数据，对地域分布的统计有一定参考意义。统计结果表明，群地点在广东省的 QQ 群组最多，达到 26.5%，其次是上海市，为 17.2%，山东省的占比为 8.5%。之后依次为河南省（6.8%）、北京市（5.1%）、江苏省（4.5%）、河北省（3.8%）、广西省（3.2%）、湖南省（2.8%）、四川省（2.5%）。

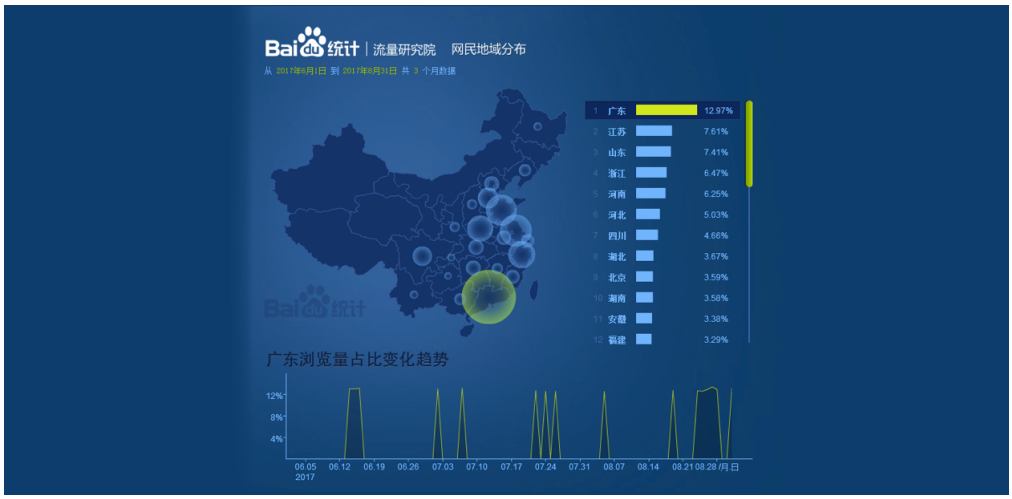
5.2.5 分析

通过对比投资类与实物、红包类两类样本，我们不难发现一些人群的特征差异，投资类群需要先进行资金投入，需要一定经济基础；而实物、红包类群的门槛则相对较低。门槛的特征反映在：

1. 投资类样本中 90 后（18–28岁）与 80 后（28–38岁）人群占比较高，而实物、红包群中的人群更加低龄化：由于没有初期的投入，00 后（0–18岁）等群体也能够轻易加入。另一方面从整体看，两类样本的主力都是 90 后（18–28岁）群体。

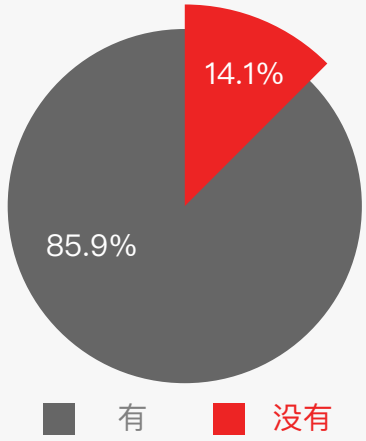
2. 两类样本中，女性用户在投资类群中的占比相比实物、红包类群的女性用户更多。二者相比，投资类群获得的收益会更多，但前期的投入也稍大。基于这样的特点，我们认为，相比男性用户，女性用户更有长远的收益计划。而在整体样本中，男性用户比女性用户多，可以认为，男性 QQ 用户更喜欢在 QQ 群中薅羊毛。

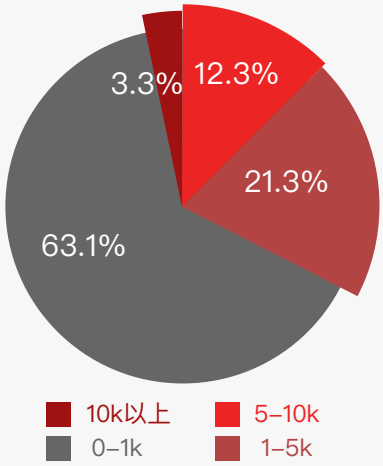
3. 从地域分布上来看，广东省的 QQ 群用户数量排在第一位，鉴于广东拥有全国最大的网民数量，我们参考了百度流量研究院提供的网民地域分析报告[2]，综合分析后发现，广东省的 QQ 群用户数量占比仍远超其网民数量比例。相比之下，群成员比例比网民占比更多的地区有：上海、山东等；符合百度统计的网民地域分布特点。



最后，我们还对部分 QQ 群成员随机提问，获得以下两点内容：

1. 通过对将近 900 名成员的问答，并对有效结果进行分析，发现有 86% 的受访者表示自己曾遭遇过骗子平台。





2.在关于 QQ 群薅羊毛月收入的回答中，63.1% 的成员表示收入在 0K – 1K之间，21.3% 的成员表示收入在 1k–5K 之间，收入在 5K–10K 的成员占12.3% ，收入在 10K 以上的成员约占 3.3%。

第六章 应对方法与安全建议

综上所述，有互联网营销活动，就有可能存在薅羊毛。但是，除了涉嫌金额较大、平台主动报警的行为外，其他行为很难定义为犯罪。因为这些薅羊毛的本质是套利，而套利从人类存在时就已经存在了。人们的社会活动需要市场，有市场才能交易商品，而商品的价格，大部分取决于商品的价值和稀缺程度。社会中的信息不对称导致商品低价买入、高价卖出，这就是最简单的一种套利行为。套利在很多时候并不违反法律，而且只要套利成本和风险小于套利所带来的收益，就一定会有人去做。

互联网厂商大多都是想通过网上营销扩大自己的用户规模，而“羊毛党”的出现很明显破坏了正常的市场秩序，对于正常的互联网秩序和社会秩序都有一定的影响。

6.1 企业应对流程

6.1.1 案例分析

案例一:

某省电信运营商移动客户端推出成长值抽取流量包的活动。设计业务流程每 10 个成长值可兑换一次抽奖机会，却因安全漏洞，被羊毛党利用充值无限流量包。

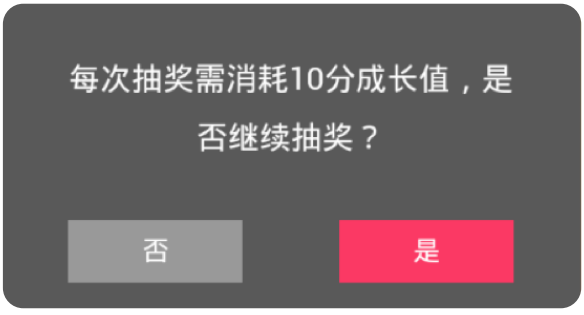
通过登录、查询、办理及商品购买等操作获得成长值，每10个成长值可兑换一次抽奖机会。奖品包含30M、70M、150M、500M、1G、2G六档流量产品。

奖品发放：

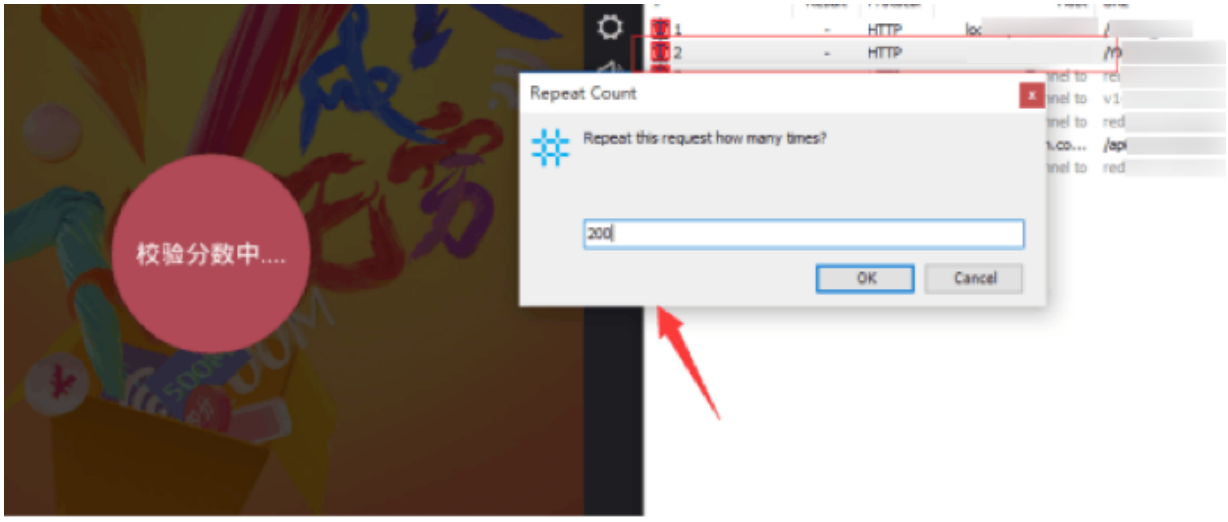
流量奖品为国内（不含港澳台）2/3/4G全网通用流量；当月有效，月底清零。

奖品将在72小时内充入中奖号码账户，请保持号码状态正常。

正常情况下，每 10 个成长值只能抽奖一次：



但其业务存在安全漏洞，抽奖过程请求包只需要并发重放便可反复抽奖，获取流量包。

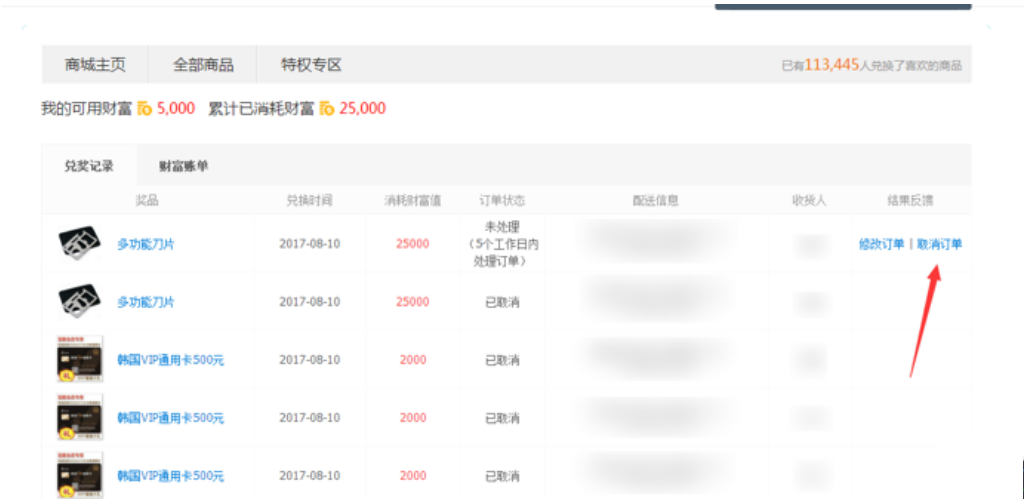


10 个成长值最终可以无限次地获取全国通用流量：

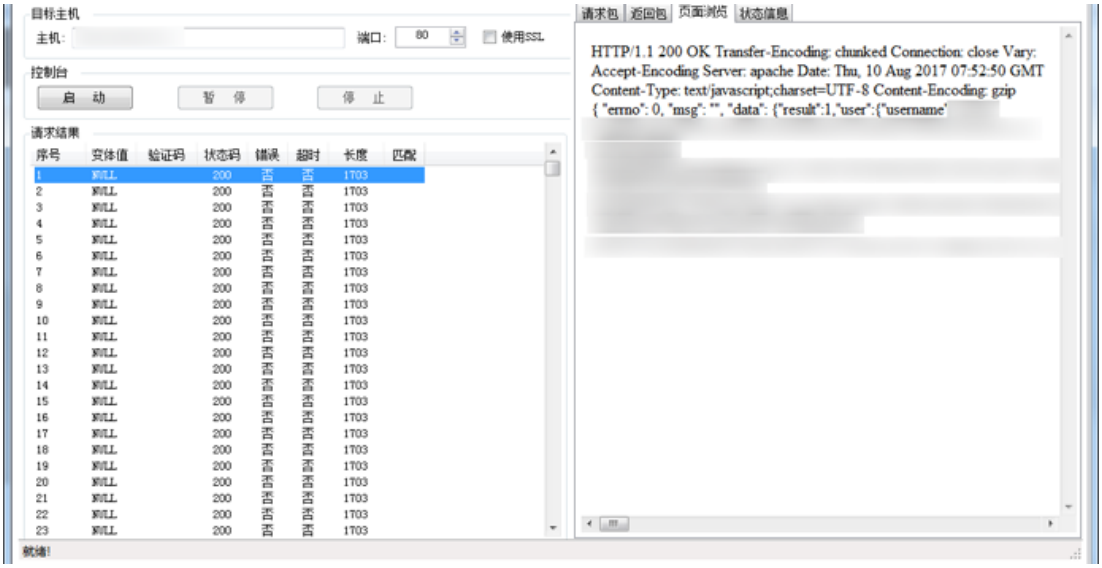
案例二:

某旅游因设计缺陷（改包重放）可刷财富值。该网站可以先使用积分兑换礼品:

取消礼品订单，会返回积分:



但是只是做了前端的删除了订单,后端并没有对多次请求取消订单做有效性验证，导致羊毛党可以使用发包工具来进行反复发送取消订单的请求，多次取消订单，进而赚取积分：



可以看到财富值已经从 5000 增长到了 30000：：

6.1.2 应对方式

针对薅羊毛的行为特点，企业可以从以下几个环节进行应对：

事前准备

待发布业务进行安全测试，除了常规的安全漏洞之外，还要尽可能发现业务逻辑上的问题并加以修复，发现实际存在的业务安全问题并在上线前及时修复，降低企业业务层面的风险。譬如，某些互金平台中，没有对用户进行四要素核验，只进行了三要素甚至两要素核验，给羊毛党留下了可乘之机。事实上，如今随着生物识别技术的发展，指纹识别、人脸识别等也都可逐渐应用到设备识别之中，加大用户登录难度，在一定程度上防范团伙性薅羊毛行为。

业务安全类问题，自动化扫描工一般难以发现，企业可以借助第三方安全厂商或白帽众测服务查找并修复。

并且，在产品设计之初应当考虑到风控的需求、特定的埋点，适当的引入第三方风控服务，能够为后续的运营和维护带来极大的便利。

具体而言，企业可通过设置单人获利上限、设置规范提醒、减少现金等直接利益、提高参与门槛、接入风控等方式，做好事前准备工作。

事中监控&响应

需要制定好两套方案，一套正常运营方案，一套应急预案。

应急预案的制定原则在于对黑产变现路径中由后向前的寻找关键节点进行门槛性限制。

针对薅羊毛用户可能发生异常的数据维度，依赖策略系统及大数据挖掘系统，建立风控策略，包括但不限于流量的网络特征、用户操作行为异常等；结合平台自身的历史数据沉淀出的黑名单，包括 IP、手机号等进行拦截。而这些，都可运用机器学习技术、合理利用所有数据，建立更完善、更自动化的风控体系。

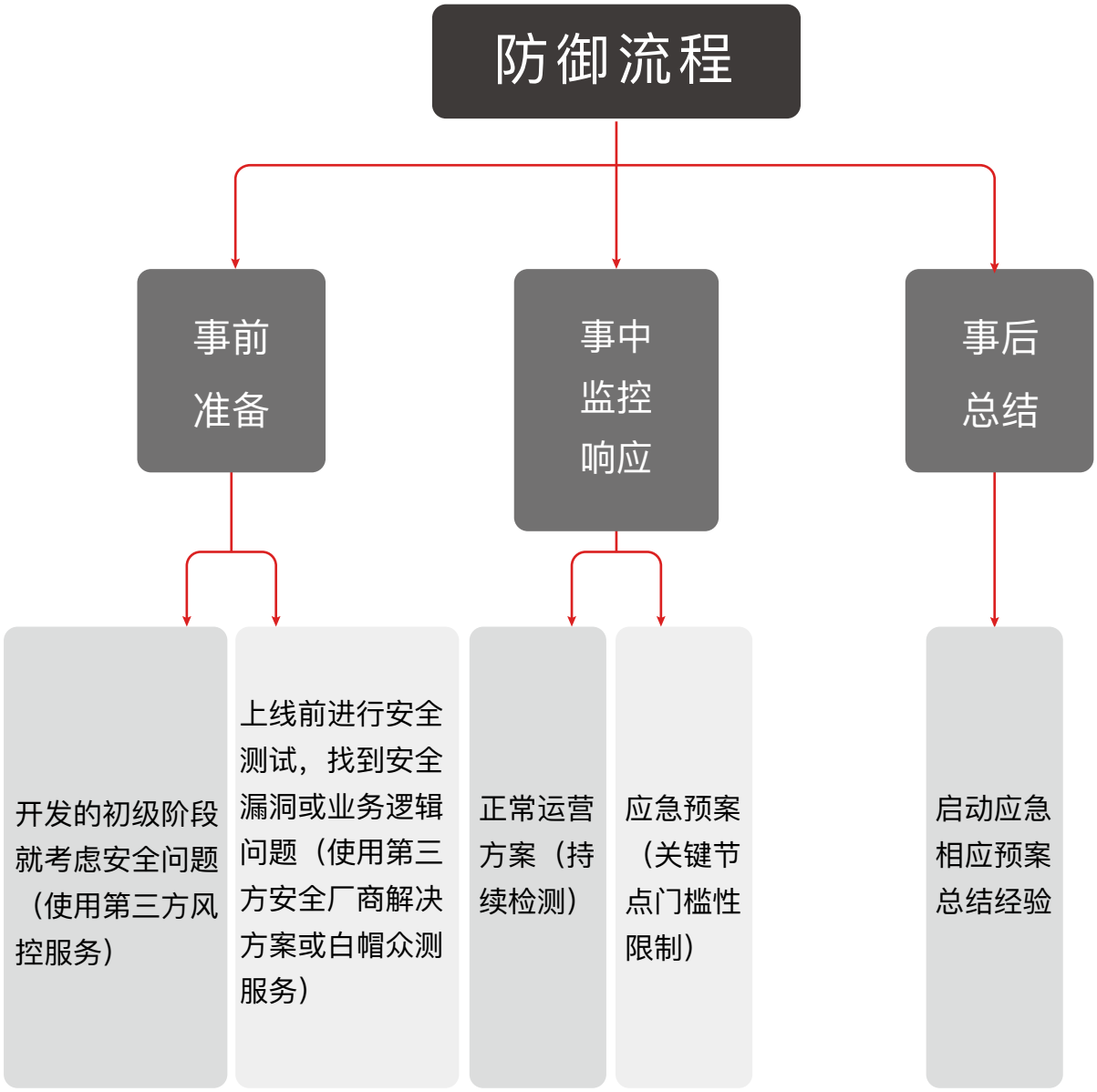
运营过程中需要做好持续监控，密切跟踪数据，一旦发现异常，需要及时进行分析和溯源，确定具体问题。必要时，启动应急预案，及时止损，保证业务的正常运行

事后总结

风险事件已经发生，首先要启动应急预案，及时修复漏洞。随后必须对本次事件中涉及到的各项问题进行经验总结，在后续的业务工作中避免出现同样的问题。

此外，风险事件中被发现的异常行为、异常账户、异常数据，都需要进行深入的分析，从中抽取出黑产所使用的 IP、手机号、邮箱、设备等信息，沉淀为风险数据名单，在此后的业务工作中，能够发挥一定的作用。

必要时，可以报警调查，并根据根据这些名单数据，追回本次风险事件所造成的损失。



此外，企业也不一定非要在“钱”上打主意，可以从多个方面思考推广方法。你的产品或商品真只有在价格上有优势吗？产品的卖点是什么，是否优良，是否吸引人，是否能抓准目标人群？推广费是否可以不直接推给目标用户而是花在其他更重要的维度上？多打磨自己的产品，有亮点，找准合适的推广渠道，制定营销策略时更加精细化，考虑的情况越多，损失也就会越少，投入资本的转换率也就越高。

6.2 合规与监管

尽管“薅羊毛”行为需要抵制和监管，但是，目前却并没有成文的规定去打击“薅羊毛”行为。“羊毛党”大多都是通过商家指制定的规则，利用技术手段获取奖品或优惠，或者通过网络手段变现，赚取差价，进行套利。羊毛党的很多活动都是在设定的游戏规则范围之内，看起来也很合理，但如今的薅羊毛团伙，却已经踏进了灰产甚至黑产的深渊。

那么，除了企业自身采取一些风控措施外，政府是否可以做些什么来规范市场环境呢？

“薅羊毛”如果在商家正常指定的规则下进行的话，那监管部门几乎很难发力，因为他们并没有越过法律这一条线。但是也不可否认“羊毛党”中还是有胆子大的人的，他们站在黑白线上，为自己的套利铤而走险。曾经有新闻报道，黑客利用某社区充值漏洞，编了拦包程序，把充值金额的 1 分钱改成 500 元，随后提交给网站，就被网站系统认可并提现。该程序在网上传播后引起大量下载，有人瞬间薅到几十万元，而该社区一夜间就损失上千万元。[3]

按照中国人民共和国刑法第二百八十六条规定：
对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。[4]

羊毛党利用网站漏洞非法牟利，很明显已经触犯了法律，同时还可构成盗窃、诈骗罪，监管部门应当加大执法力度，以儆效尤。

2017 年 8 月，成都商报报道了某“黄家三姐妹”利用某电商平台的业务逻辑漏洞，申请“七天无理由退货”但事实上并未寄还货物，而是提供虚假单号获取退款。最终因涉嫌诈骗而倍警方抓捕。[5]

因此，监管机构出台的相关法律对于那些跨越法律线的“羊毛党”而言，其实可以起到约束作用。这也要求监管部门加强追踪力度，不“懒政”，多部门相互配合，严惩违法者。在恶意“薅羊毛”事件发生后，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。

6.3 薅羊毛产业链背后的社会问题

第四章的数据分析内容显示，薅羊毛 QQ 群中 90 后和 00 后占比分别为 37.8% 和 35.5%，这个年龄段基本上是青少年，正是读书的好时候。薅羊毛虽然是一种套利的手段，但其所消耗的时间成本要远远高于所获得的利益。在最应该努力学习的阶段浪费大量的时间在这些小利上，未免得不偿失。教育部门应加强对青少年的法律意识和道德观教育，对其正确引导，把聪明才智用在更好的地方。

因此，监管机构出台的相关法律对于那些跨越法律线的“羊毛党”而言，其实可以起到约束作用。这也要求监管部门加强追踪力度，不“懒政”，多部门相互配合，严惩违法者。在恶意“薅羊毛”事件发生后，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。

6.3.1 教育资源分布不均

第四章的数据显示，虽然群成员地域分布显示北京占比很高，为 5.51%，但剩下的绝大部分群成员还是分布在其他省份。我国人口众多，面临的问题也很多，教育资源不平等的问题尤为严重。根据 2015 年的《中国留守儿童心灵状况白皮书》，全国妇联曾根据中国 2010 年第六次人口普查资料样本数据推算出全国有农村留守儿童 6100 多万，占农村儿童的 37.7%，占全国儿童的 21.88% ；根据联合国儿童基金会的数据，其中大约 4300 万的留守儿童在 14 岁以下。[6]这也许是有史以来最大的一个留守儿童群体，他们的数量相当于英国、法国全国的人口总数。处在非一线城市的青少年可能无法获得一线城市那样优越的教育资源，我们不能正确评估他们的受教育水平，也无法对他们的生活做出评判。但是，沉溺在薅羊毛 QQ 群里，很容易让他们染上网瘾、贪小便宜 、投机取巧、不思进取。政府和社会都有责任将他们从薅羊毛这种灰产领域引导出来，也有责任扶正他们的三观，加强教育资源的投入，避免他们越陷越深甚至走向犯罪。

教育公平是社会公平之本，是实现社会公平的伟大工具。农村留守儿童教育问题的解决不仅关系到我国教育公平的实现，也关系到社会主义新农村的建设和社会公平的实现。只有坚持用科学发展观统领教育事业工作全局，努力做到“让每个人享有出彩的机会”，才能造就数以亿计的高素质劳动者、数以千万计的专门人才和一大批拔尖创新人才，建设规模宏大、结构合理、素质较高的人才队伍，开创人才辈出、人尽其才的新局面。

6.3.2 社会监管有待加强

在第四章的 QQ 群数据分析中，北上广等地的 QQ 群用户占比不小。北上广作为中国的一线城市，拥有最多的网民数量和外来人口数，会有一部分人存在不劳而获、贪小便宜、投机取巧的想法，他们自身的素质和教育程度也并不是很高。利用网络薅羊毛简单便利，成为这些人的首选。相信很多人都看过“三和大神”的报道，有一群人不愿意找正式工作，蜗居在深圳这个大城市名为“三和”的角落里，出售身份“做法人”、“做贷款”、“做P2P”、“做取现”（蚂蚁花呗、信用卡）、出售银行卡和手机、甚至卖身份证度日。[7]所有这些业务都多少涉及灰色产业，其中做贷款、做 P2P、做取现等，都与薅羊毛有关。这种现象引人深思，政府需要对此加强监管，一方面要进行社会教育、引导正确的社会风气，另一方面要清理这些无业游民聚集区，提供更多岗位、积极促进就业。

6.3.3 公民法律意识淡薄

在我们前面的调查中，有几名群主其实是大学生，他们不仅自己开发各种黑客工具，挖洞赚钱，甚至还进行身份信息（姓名、身份证号、手机号、银行卡等）的买卖。他们并没有认识到自己做的事情不正确甚至触犯法律，价值观存在一定偏差。这在一定程度上反应了当代年轻人法律意识的淡薄。

《网络安全法》第二十二条规定：
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。[8]

薅羊毛中有一部分人是在运营商的规则下“合理”薅羊毛的，但也有一部分人已经站在了法律的边缘。加强《网络安全法》及的实施及后续更详细法律法规的的制定、实施与普及，相信会改善这类问题。

6.4 小结

薅羊毛本是黑色产业链中的冰山一角，甚至严格来说更偏向灰产。当我们认真取证，剖析之后，能发现它在黑产之外也已经逐渐发展成了一种社会现象。整个产业链背后，其实还有更多值得我们反思的东西。

一种社会现象的背后往往存在错综复杂的利益关系，只修复其中一环也很难改善大局。要想完全解决问题，需要社会各界的通力合作。对于企业来说，不仅要采取合理的防御应对措施，也要意识到自己应当担负起相应的社会责任。比如现在很多企业已经在开展”校企结合“活动，将教育与就业紧密联系起来，就是很好的实践。而对于政府和教育部门来说，出台、细化政策，落地实施，加强监管也十分重要。而从这个产业链中涉及的技术角度来说，如今我们都在关注新技术的发展与落地，却不想在这方面，攻击者比防御者走得更快更远。网络安全没有银弹，每个人都只能不断向前。

社会是个万花筒，当你变换角度，总能看到不一样的色彩。有明亮艳丽，就有灰暗阴沉。忽视和逃避都不能解决问题，单纯的批判也毫无意义。只有正视、承认这些问题的存在，了解问题背后的原因，才能想办法减少黑暗，增加光明。

附录

参考来源

[1]《第40次中国互联网络发展状况统计报告》，CNNIC
https://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/201708/P020170807351923262153.pdf

[2]《网民地域分布报告》，百度流量研究院
http://tongji.baidu.com/data/district

[3]《一夜之间羊毛族撸走上千万 快操盘平台声明:触犯法律》，新浪财经
http://finance.sina.com.cn/stock/stockaritcle/20151111/092323737004.shtml

[4]《中华人民共和国刑法》 ，中华人民共和国公安部
http://www.mps.gov.cn/n2254314/n2254409/n2254410/n2254417/c3701295/content.html

[5]《网购后办假退货 诈骗1300余件商品》，成都商报
http://e.chengdu.cn/html/2017-08/22/content_603903.htm

[6]《中国留守儿童心灵状况白皮书 （2015）》 ，上学路上儿童心灵关爱中心，北京师范大学
https://wenku.baidu.com/view/1206d2ef4b35eefdc9d333a4.html

[7]《在三和玩游戏的人们》，触乐网
http://www.chuapp.com/article/282974.html

[8]《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

关于报告

作者

FreeBuf 研究院：

鲍弘捷、曾裕智、朱嘉豪、王鹏、朱伊琳、余桂茗

同盾科技反欺诈研究院：

祝伟、丁杨、章岚、李克勤、高岳、江杰、杜鹃、赵宇琦

美术设计：

贾召霞

深渊背后的真相之「薅羊毛产业」报告

同盾科技
www.tongdun.cn

FREEBUF
WWW.FREEBUF.COM