Broadview
www.broadview.com.cn

风控要略

互联网业务反欺诈之路

马传雷　孙奇　高岳　著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

Broadview®
www.broadview.com.cn

风控要略

互联网业务反欺诈之路

马传雷　孙奇　高岳　著

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

作者简介

马传雷

曾任同盾科技反欺诈研究院执行院长、广州中国科学院软件应用技术研究所电子数据取证实验室特聘专家，还曾担任腾讯安全应急响应中心技术负责人、绿盟科技安全技术部总监等职务，国内知名安全专家。

孙　奇

曾任同盾科技反欺诈产品研发总监，浙江大学硕士，知名Java架构师、Qcon全球开发者大会讲师。

高　岳

东南大学硕士，曾任同盾科技移动安全产品研发总监，也曾在腾讯安全平台部负责移动产品安全检测能力建设和安全产品研发，业务安全专家。

版权信息

COPYRIGHT

书名：风控要略：互联网业务反欺诈之路

作者：马传雷等

出版社：电子工业出版社

出版时间：2020年8月

ISBN：9787121392788

字数：387千字

内容简介

这是一本全面描述互联网业务反欺诈体系的书籍，本书主要分为洞察黑产、体系构建、实战教程和新的战场4个部分。第1部分介绍了黑产欺诈团伙的运作套路和攻击手段；第2部分总结了我们在构建反欺诈技术体系过程中沉淀的实践经验；第3部分分享了我们和黑产对抗的多个实战案例，以及机器学习算法的综合运用；第4部分介绍了我们在物联网、内容安全、隐私合规等方面的实践和对海外厂商的观察。

读者通过仔细阅读本书，可以对互联网反欺诈的过去、现在和未来有一个系统的认识。希望本书能够为正在关注该领域或从事相关工作的读者提供有价值的参考。本书适合互联网投资人、创业者、产品经理、运营人员和安全风控人员阅读。

前言

从2018年开始，我和高岳、孙奇一起从事业务安全产品设计、研发的工作。在此之前，高岳是移动安全方面的专家，孙奇是资深的Java 架构师，而我则是从事黑客攻防对抗的工程师。于我们而言，这是一段非常美好的经历，非常感谢命运的安排。

因为个人兴趣和工作需要，我们和很多朋友就互联网业务安全进行了深入交流。他们有的是互联网公司的产品研发人员和运营人员，有的是传统金融机构互联网线上业务拓展推广人员，也有的是专业风控和安全从业者。从与他们的沟通交流中，我们学到了很多业务领域的知识，同时也发现大家对互联网黑产及互联网业务安全体系构建缺乏深入了解。我们常常听到这样的话：“投入了很多资源构建互联网业务安全体系，购买了专业公司的风控产品和服务，但是依然没能阻止网络黑产无情的攻击。”

在实际项目中，我们也遇到了一些困扰：产品POC 测试严重脱离业务场景实际需求，错误的策略部署导致产品无法正常发挥防御能力。我们在复盘时常常反思这些问题，是不是可以通过某些方式帮助客户更全面地理解业务风险的脉络和黑产攻击的套路。很多问题的产生并不是因为黑产团伙的技术有多么高明，而是因为防御方不能够很好地帮助客户理解业务风险。

2019年3月的某一天，高岳提议写一本全面介绍互联网业务反欺诈体系构建和实践经验的书籍，这个建议点燃了我们心中的火焰。我们立即开始整理资料并写作，经过8个多月的努力，我们在2020年的春节前完成了这本书稿。

本书主要分为洞察黑产、体系构建、实战教程和新的战场4个部分。第1部分介绍了黑产欺诈团伙的运作套路和攻击手段；第2部分总结了我们在构建反欺诈技术体系过程中沉淀的实践经验；第3部分分享了我们和黑产对抗的多个实战案例，以及机器学习算法的综合运用；第4部分介绍了我们在物联网、内容安全、隐私合规等方面的实践和对海外

厂商的观察。

希望读者通过阅读本书，可以对互联网反欺诈的行业现状有一个系统而具体的认识。业务安全的真正力量是内生的，专业的安全风控公司可以提供工具、平台和策略建议，但是只有业务方真正理解风险和防控思路，才能在与黑产的对抗中设计好业务规则、运营好安全策略，取得较好的效果。如果读者正在关注该领域或从事相关工作，我们相信本书一定能够为您提供帮助。

我们相信本书将成为中国互联网历史中一个微小但坚硬的符号。以当前互联网的进化速度，若干年后本书介绍的风控体系可能会被新技术完全重构，行业态势也会有很大的不同。后来者可以通过本书观察和体会行业与技术的演进轨迹，进而把握未来的发展趋势。

用工作之外的时间把自己的想法变成数十万字的图书，是一件非常考验耐心的事情。除了三位主要作者，还有以下几位同学坚持参与撰写本书的部分内容。

· 李克勤、章岚撰写了“第2章　黑产武器库概览”、“第10章　黑风险数据名单体系”和“第11章　黑欺诈情报体系”章节的初稿。

· 郭嵩、彭亮撰写了“第4章　黑风控核心组件设备指纹”中Web 设备指纹和JS 混淆相关内容的初稿。

· 赵峰撰写了“第5章　基于用户行为的生物探针”章节的初稿。

· 江杰撰写了“第6章　黑智能验证码的前世今生”章节的初稿。

· 贺海军、王明英撰写了“第12章　黑机器学习算法的使用”实战案例相关的内容。

· 刘莹撰写了“第13章　黑互联网反欺诈实战”章节的初稿。

在稿件完成之际，有特别多想感谢的朋友。在过去的一年中，罗小果等同事运作的项目，促使我们对业务安全防御体系有了更深入的思考，使得本书的整体框架更具有逻辑性。在完成初稿后，陈钧衍等多位技术同事给出了很多非常好的修改建议。感谢电子工业出版社的策划编辑符隆美，感谢我们的同事韬哥、伟哥、艺严等，感谢“蓝星技术群”的互联网安全同行，没有你们的鼓励和帮助，也许就不会有这本书的面世。

作为互联网安全从业者，回顾这几年走过的路，黑产的技术发展和规模膨胀给我们带来了很大的压力，同时也让我们有了更大的动力去构建更加有效的安全防御产品体系。在此我们向互联网安全行业中诸多提携我们成长的前辈和守望相助的朋友们致敬，他们是alert7、binw、cnhawk、coolc、cy07、flashsky、huiwang、instruder、kevin1986、lake2、lenx、linkboy、marcohp、mkliu、oldjun、pix、rozero、scz、tb、xi4oyu、xundi、方斌、丁丽萍、顾孔希、高亮、何艺、刘进、林鹏、马坤、聂君、秦波、王彬、王任飞、王英健、阎文斌、杨珉、赵弼政等等（排名不分前后），还有很多很多行业拓荒者和同行者，在此难以一一列举。

由于作者写作水平有限，书中难免存在疏漏与不足之处，恳请读者批评指正。就本书覆盖的内容而言，在反爬虫、反洗钱、业务生态秩序安全治理及用户安全心智建设等深水区没有进行深入阐述，我们也是心有遗憾并且希望能够在下一本书中弥补，敬请期待。

马传雷

引言　互联网业务安全概述

当前中国互联网安全产业大体可以分为基础安全和业务安全两个领域。纵观中国互联网安全20多年的发展过程，业务安全还是一个相对年轻的细分领域。如果以上市为创业成功的标准，那么业务安全领域的企业还在向着成功的方向努力奔跑着。

从互联网诞生至2014年，互联网安全行业关注的热点基本都聚焦在网络安全、系统安全和应用安全这三大基础安全领域上，“DDOS”（分布式拒绝服务攻击）、“漏洞”、“拖库”和“挂马”等大家耳熟能详的术语也是从这些领域中衍生出来的。启明星辰、绿盟科技、奇安信和深信服等比较知名的企业，都属于基础网络安全领域。行业的发展以合规需求、漏洞攻防技术发展为驱动力，缓冲区溢出攻击的流行推动了IPS 产品的发展，CC 攻击的兴起促使Anti-ddos 产品成为企业网络安全的防护产品，SQL 注入攻击技术的普及则让WAF 产品成为安全防御体系的标配。专业的乙方安全公司和“在野”的黑客团伙是这一时期较为主要的技术博弈方，而绝大部分企业和政府单位的安全防护体系建设均以采购和使用乙方安全公司成熟的商业产品、解决方案和外部安全服务为主。

2014年前后，随着互联网业务的爆炸式发展，黑产团伙开始从“攻击渗透系统获利”的传统套路进化到“利用业务风控缺失进行大规模牟利”的模式，并且逐渐形成规模庞大、分工明确的黑色产业链。同一时间，一批业务安全风控企业横空出世，标志着业务安全细分领域的崛起。在此之前，仅有一些大型的互联网公司因为黑产对其核心业务进行激烈的攻击而成立了专业的业务安全团队，如腾讯的QQ 账号安全团队和盛大游戏的反外挂团队。这些团队仅在公司内部做了很多拓荒性的工作，设计和研发了一些出色的内部安全平台和工具，但是对整个互联网业务安全领域的影响不足。而一批新兴的乙方风控企业，则选择惠及更多的企业，将技术算法赋能给其他风控能力薄弱的互联网公司，共享黑产对抗成果。

在2014年之后的几年时间里，互联网风控反欺诈阵营和黑产集团展

开了波澜壮阔的鏖战，涉及游戏、电商、支付、视频直播甚至共享单车等几乎所有互联网业务领域。双方在拉锯战中互有胜负，直到公安机关“净网行动”全面展开后，黑产的嚣张气焰才得到有效遏制。

黑产攻击的蔓延

从近年来的多个黑产攻击事件的分析和深度追踪中，我们可以看到黑产已经全面渗透到互联网平台及金融机构的各个场景，迅速在全网蔓延，近几年呈现出愈演愈烈的趋势，给企业和社会造成了不可估量的损失。据统计，国内黑产成员超过50万人，黑产团伙之间已经形成了相互分工、紧密合作的产业生态。由于企业之间信息和数据的割裂，欺诈分子往往能顺利游走于不同平台之间。

从公安机关已经侦破的黑产案件来看，黑产的攻击规模不断扩大，涉及的互联网企业和用户也越来越多。2017年，浙江省绍兴市警方侦破了一起非法窃取30亿条用户数据的黑产攻击案件。犯罪团伙利用技术手段非法劫持运营商流量，进一步利用大数据分析技术获取用户在网上的搜索记录、出行记录、开房记录、交易记录等信息，用于对互联网金融企业的进一步攻击。我们为网上银行提供的账号保护SaaS　服务数据变化趋势如图1所示，可以看出黑产团伙对金融业务的攻击风险也呈现规模不断扩大的态势。

近几年来，互联网领域发生了多起黑产攻击事件，都印证了我们对黑产发展态势的判断。表1是我们收集的一些典型的黑产攻击事件，供读者参考。

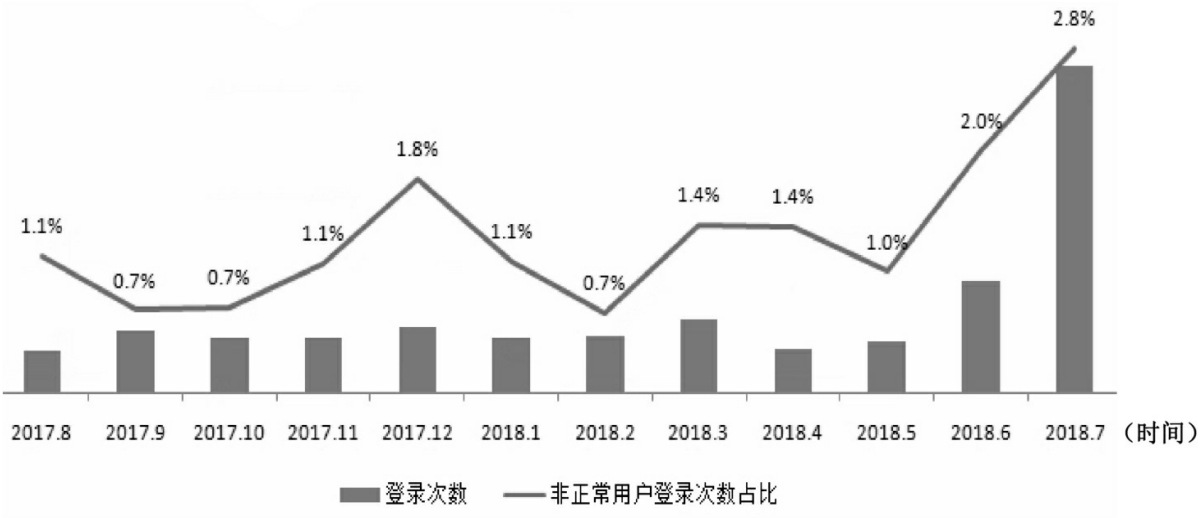

图1　登录场景风险分布

表1　典型的黑产攻击事件

年　份	事　件	过　程
2017 年	“快啊答题”黑产团伙破解多家互联网公司验证码	“快啊答题”黑产团伙开发的验证码破解软件，采用先进的基于神经网络深度学习的人工智能技术，可不断自我训练学习以完善准确度，快速海量地破解验证码。该团伙仅一个季度就对多家互联网公司的验证码进行了数百亿次破解，非法获取并贩卖大量公民信息，已在 2017 年被浙江省绍兴市警方破获
2018 年	星巴克圣诞特饮邀请券被黑产“薅羊毛”	2018 年，星巴克推出营销活动：下载星巴克 APP，注册后可获赠一张邀请券，能免费兑换任意一杯中杯圣诞当季特饮。由于此次营销活动没有采用反羊毛措施，黑产开发了自动注册机，后台自动调用打码平台进行自动兑换，短时间获取的廉价兑换券高达数十万张。换来的兑换券通过朋友圈、微商等渠道批量销售。在朋友圈中，价值 25 元的咖啡券以 9.9 元、8.8 元，甚至两三元的价格进行销售。随着消息的扩散，“薅羊毛”的行为呈指数级增长，开始出现网友在星巴克咖啡厅排队兑换咖啡的场景，部分店面的正常用户消费受到严重影响
2018 年	浙江省绍兴市警方侦破“瑞智华胜”窃取 30 亿条用户账号数据案件	浙江省绍兴市警方侦破了新三板上市公司北京瑞智华胜科技股份有限公司（简称“瑞智华胜”）非法窃取用户 30 亿条信息的案件。这次案件信息窃取规模庞大，涉及多家互联网科技公司，包括百度、腾讯、阿里、京东等全国 96 家互联网公司。该涉案团伙通过与全国十余省市多家运营商签订营销广告系统服务合同，非法从运营商流量池中获取用户账户信息，从而操控用户账号，在微博、微信、QQ、淘宝和抖音等平台上加粉、加群、违规推广，非法获利

续表

年　份	事　件	过　程
2018 年	“xxtouch”团伙恶意注册养号	“xxtouch”是一款按键精灵，它集成了改机工具的功能，包括伪装手机信息、GPS 信息功能均可轻易一键伪造，为恶意注册黑产配备了全套武器。该黑产团伙形成了“下游微信恶意注册养号人员——中游脚本开发人员——上游软件开发人员”的全链条，现已被警方破获
2019 年	巧达科技非法窃取数亿条公民信息	2019 年，号称拥有全国最大简历库的招聘类数据公司巧达科技被曝公司所有人员被北京警方带走。该公司从国内各大招聘网站窃取和整合了多达 2.2 亿份自然人简历，其中包含大量的个人隐私信息

业务安全的崛起

黑产在互联网领域的横行无忌，从反面推动了互联网业务安全反欺诈领域的快速发展。互联网业务模式的不断创新决定了风险的复杂多变，如今业务安全行业的技术、产品和解决方案，已经覆盖了几乎所有的互联网业务常规场景，并且和传统安全领域也发生了深度的交集和融合。

下面是常见的风控场景举例：

· 注册和登录场景的风控：如何对抗黑产注册虚假账号、养号的行为，如何对抗黑产暴力破解账户密码，如何对抗“撞库”攻击。黑产手中掌握了大量的手机号卡、公民信息和数以亿计的已泄露的互联网账号密码，这对任何一个互联网平台都是致命的威胁。

· 营销活动风控保护：营销活动发放的红包、游戏点券或其他奖励如何才能够不被黑产团伙“薅羊毛”。这类事件层出不穷，互联网上也常有报道。

· APP 渠道推广保护：推广APP 装机量投入巨额费用后，如何衡量真实效果。用户每安装激活一个APP，平台需要支付10元甚至20元，黑产通过“手机农场”虚假安装已经是广告行业顽疾。

· 交易和支付场景风控：盗号支付如何解决、非法聚合支付如何解决、洗钱如何解决，这些合规性问题关乎支付平台和相关业务的生死。

· 接口安全保护：短信发送接口被坏人用于制作“短信炸弹”是大家都遇到过的场景。

· 内容安全：内容安全既包括“入”也包括“出”，“入”是检测用户发布到平台的内容是否包含“色情、反动、赌博和暴恐”等违规信息，“出”则是对抗专业爬虫大量获取网站内容信息。

在这些场景中，黑产具备哪些资源、是如何实施攻击的，互联网企业如何从数据、工具和算法等多个维度展开对抗，我们将在后续章节进

行详细的讲解。

第一部分　洞察黑产

第1章　黑产发展态势

本章将介绍国内黑产的总体发展情况，供读者参考。值得一提的是，公安部在2019年的“净网行动”对黑产生态进行了系统性的打击，黑色产业链在经历了5年多的野蛮发展之后，终于得到了有效地遏制。

1.1 黑产组织结构

根据中国互联网络信息中心在2019年8月发布的《第44次中国互联网络发展状况统计报告》，截至2019年6月，我国网民规模已达8.54亿，手机网民规模已达8.47亿。

如此大规模的互联网用户群体产生了巨大的互联网业务需求和交互流量，形成了两个互联网生态，一个是看得见的，另一个是看不见的。看得见的生态，是互联网厂商用网站、APP、小程序和线上线下的服务构建起来的。它是由很多优秀的产品团队设计产生的，有监管、有秩序、有规则。看不见的生态，是围绕主流互联网产品和服务衍生出的一条条黑灰色产业链，聚集了规模庞大的黑产群体。普通网民看不到它的形态，但是却真实存在并且拥有强大的力量。

黑产群体组织分工明细，如有“羊头”、“推手”和“羊毛”之分的羊毛党群体（后文我们会详细介绍这些术语），并且善于伪装。黑产从业者有全职或兼职，在兼职人群中，有各行各业人员，辨认难度大。同时黑产群体技术更新迭代迅速，可以在短时间内对厂商的防护手段破解并更新多个版本的作弊工具。据不完全统计，在这个庞大的黑色产业链条中，黑产从业人员已达数十万余人，每年给互联网公司造成的经济损失超过百亿元。

黑产群体有各种各样的工具，利用这些工具极大地提升了黑产作案效率，同时也更加扩大了企业厂商的危害。这些工具往往是为了某种特定的应用场景而设计的，被黑产发现之后，开始大规模利用，对互联网带来了巨大的影响。

经过长期对黑色产业链的跟踪调查，我们整理出了黑色产业链结构，如图1.1所示。

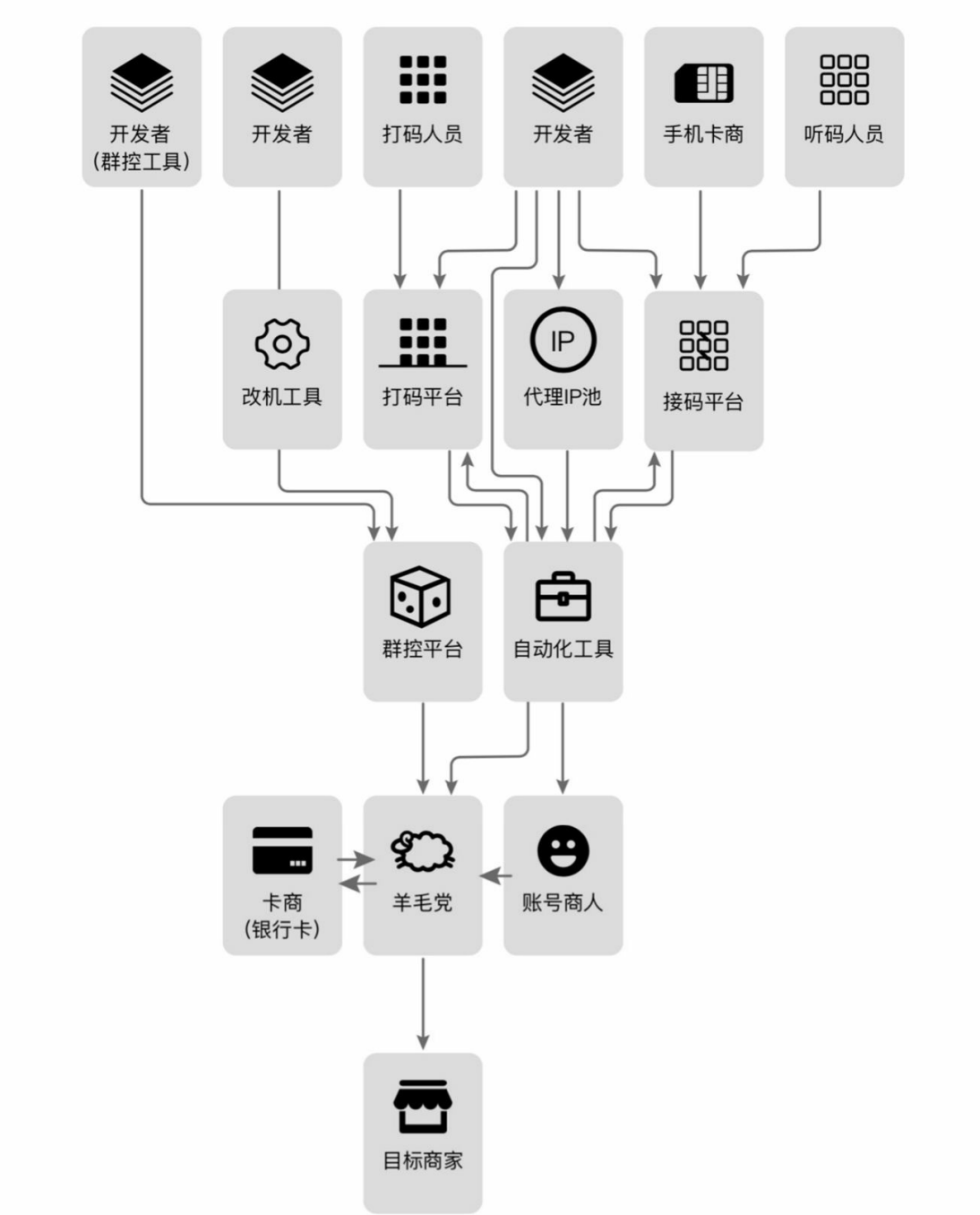

图1.1　黑色产业链结构

在整个黑色产业链中，各个环节都已有专业分工，相互之间紧密配合，其中技术类黑产负责提供丰富的代理IP、虚假号码和各类自动化工具。

互联网黑产远不止羊毛党一种，只是很多自媒体会把参与营销、优

惠、满减活动并以此牟利的黑产统称为羊毛党。在业务安全的视角上分析，我们会把不同行业、不同场景中的风险行为分门别类，针对特定的风险，使用特定的规则或模型进行防控。

在此，我们整理了一份“反欺诈词典”，用于定义各类黑产的具体行为和名词术语，列举如下：

· 垃圾注册：在注册环节中，使用虚假、不稳定的身份信息，如虚假号码、通信小号、临时邮箱、虚假邮箱注册，或者使用脚本、注册机进行批量注册的行为，称为垃圾注册。注册完的垃圾账号，在直播视频行业中被用于关注、点赞、观看视频量、批量评论等，在电商行业被用于刷店铺访问量、关注量等。此类账号在账号命名上也有所特征，常见的有不规则英文组合、古诗词句截取等。

· 薅羊毛：使用虚假身份信息或自动化工具参与各类营销活动的行为，营销活动包括但不限于折扣、返现、抽奖、满减等形式，并且不能给平台带来实际的活跃用户或订单交易。执行薅羊毛行为的人称为羊毛党。

· 黄牛/刷单：在合法销售途径以外，垄断、销售限量参与权或商品，并以此牟利的中介人称为黄牛。从业务安全的视角上看，黄牛和刷单在行为上相似度极高，都发生在交易场景中，并且具有爆发性，会大量使用自动化工具。黄牛和刷单的区别在于，刷单过程中买到的产品，即使加价出售，也比商品原来的价格要低。而黄牛在倒卖的时候，价格会远高于商品原本的价格。还有区别在于价格和目标商品类目上，在刷单过程中刷手需提前确认收货好评垫付商品金额，为了控制刷单成本一般选择低价商品。但黄牛的目标多为热门稀缺的热点商品，便于后期加价出售获利。如某热门手机，某海外热门歌手演唱会门票每年必遭黄牛哄抢，单价商品倒卖价格已达上万元。在智能风控引擎中，这两种欺诈行为的表现几乎是一致的，不做详细区分。

· 众包：由多个独立的个体共同参与完成的一项任务被称为众包。有羊头发起，众多羊毛党在线参与的薅羊毛行为称为众包薅羊毛。一个典型的案例，在某微信群中，羊头和羊毛党配合，羊头负责收集线报并同步到微信群内，一般是商品折扣或满减形式。同时，羊头在群内收购商品，羊毛党参与活动，低价购买了商品，可以直接转售给羊头，羊头支付商品成本和手工费用。羊头借此囤积了大量的低价商品，再通过其

他线下渠道转售出去。所有参与此次薅羊毛行为的用户都是独立的真实用户。

· 炒信：通过各种途径和手段进行虚假交易，快速提升商户交易量、信用等级的行为统称为炒信。

· 套利：由商户端发起的薅羊毛行为被定义为套利。例如，在银联活动中，某家银行的活动形式是，用户到指定门店消费，消费满100元返50元，同时商户也可以获得50元奖励。活动期间出现了商家和羊毛党联合欺诈，羊毛党到店扫码支付，商家会退回支付的钱，没有发生任何实质上的交易，但是羊毛党和商家都能够获得奖励，以此骗取奖励。

· 空包：虚假发送快递，发送空的快递或包裹。在电商场景中，订单提交后，商家将商品打包，通过快递方式发送给用户。在套利或炒信时，商家必须给平台提交物流单号完成发货动作，买家签收后钱款打入卖家账号，一笔交易才算完成。此时，如果商户选择发送空的快递，或者提交已经完成的、其他平台的快递单号，则可以节约成本。市面上也有很多打着代发快递名头的空包网站，代发一单快递的售价为0.6元～0.8元，并且可以提供真实的物流信息来规避甲方平台的风控策略。

以上仅列举了一些常见的、在黑产中间已经比较成熟的行为术语。这些名词对于从事互联网风控和业务安全的读者来说，应该都不陌生，每一类业务风险在不同的行业中都会有不同的表现。还有很多欺诈行为是隐性的，需要长期监控和挖掘才能发现。

1.2 黑产成员分布

我们的情报团队采用基于人工智能的情报系统对黑产网络进行了布控，对黑产团伙的运作方式、人员分布等进行了深入跟踪和分析（黑产情报系统的运行机制如图1.2所示，我们在后面章节会详细介绍）。

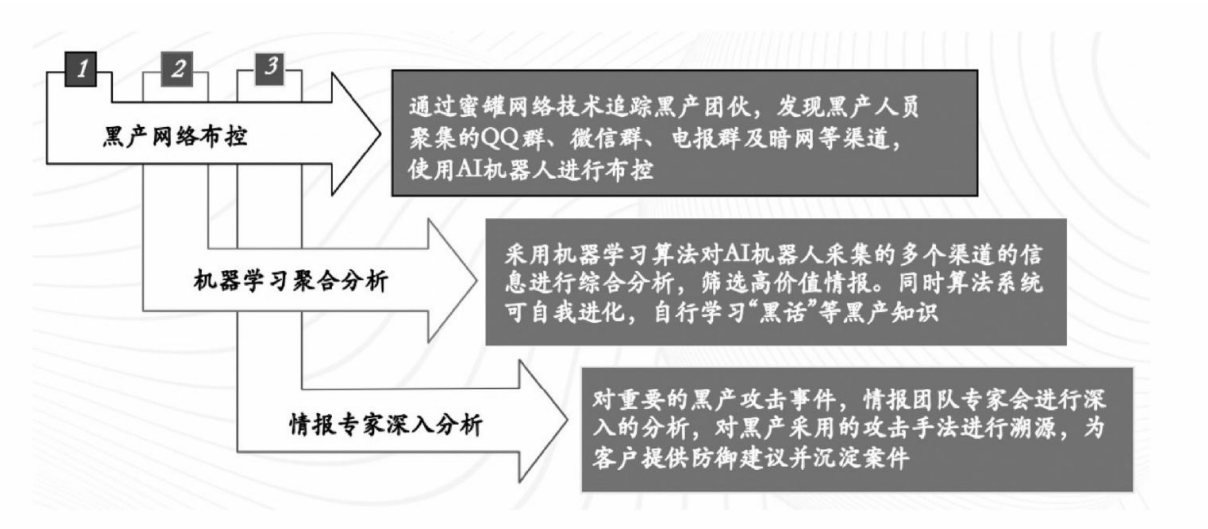

图1.2　黑产情报系统的运行机制

通过取样近万名活跃黑产参与者进行分析，结果如图1.3所示，其中年龄为18岁～24岁的参与者占比超过50%。

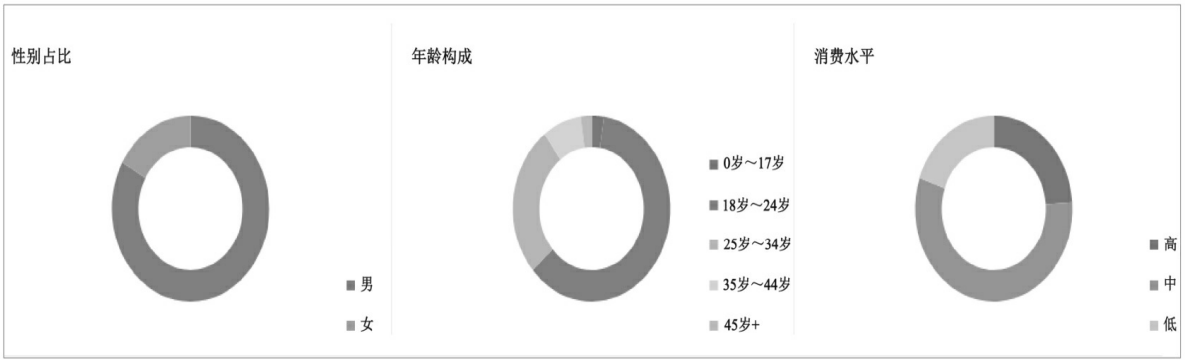

图1.3　黑产参与者分布

1.3 黑产专业化分工

在金钱驱动下，黑产团伙的分工越来越精细，专业化程度不断提升，大数据分析、深度学习和人工智能技术也被广泛使用。

2017年，浙江省绍兴市警方破获了“快啊答题”打码平台非法获取贩卖公民信息案。该团伙利用人工智能进行晒密撞库、分销数据、冒充诈骗、洗钱，构成了一条完整的黑色产业链。该案件受害人遍布全国20多个省、5个自治区、4个直辖市，涉案金额高达2000多万元。在该案中，黑产团伙中的技术人员基于主流人工智能深度学习Caffe框架，使用vgg16卷积核神经网络模型，研发了一套非常先进的验证码自动识别平台，总累计破解验证码约1200亿次。

1.4 黑产攻击规模

据互联网上一些公开的统计信息，各类黑产每年给互联网公司带来的经济损失已经超过百亿元，黑产从业人员高达数十万人。这些信息的数量级基本是符合的，我们从SaaS 服务调用数据也可以对黑产的规模有一个直观的认识，如图1.4所示。

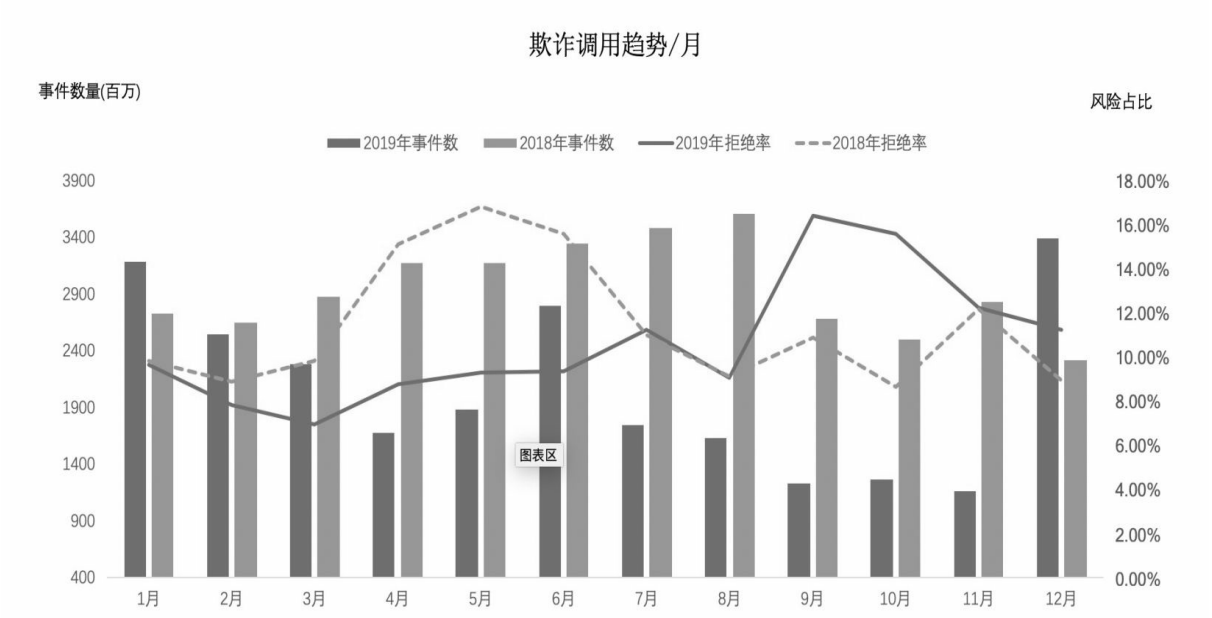

图1.4 反欺诈服务调用趋势

图1.5是各类事件中风险事件占比，一般为10%～15%。这个数值与行业、场景、时间有直接的关系。其中，电商平台在“双11”、“双12”和“6·18”等大规模的促销活动时段，优惠力度比较大，欺诈事件会比其他时段要多。黑产团伙一般也不打无准备之仗，往往在活动之前一到两个月就开始筹备，注册账号、养号、开发和测试作弊工具等行为都会提前进行。

从不同业务场景来看，注册登录场景中的风险占比是最高的，可以高达40%。因为对于绝大部分的业务流程来说，注册登录是所有后续业务的门槛。黑产必须迈过这个门槛，才能执行交易、支付等行为。因

此，如果能够在注册登录场景中做好风控，把绝大部分的黑产拒之门外，在后续的其他环节中，风险就会降低很多。

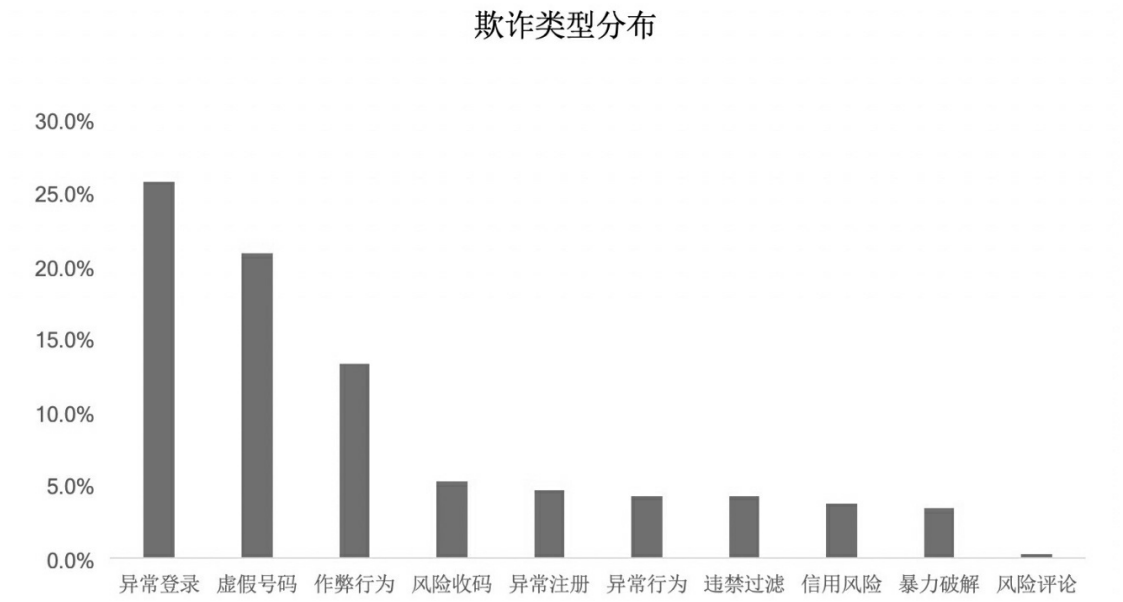

图1.5　欺诈类型分布

从地域上看，如图1.6所示，欺诈攻击的来源主要集中在华东地区，占比为45.72%。这并不代表黑产真实的所在地，而是通过IP　归属地、手机号归属地、设备定位等信息综合得出来的。

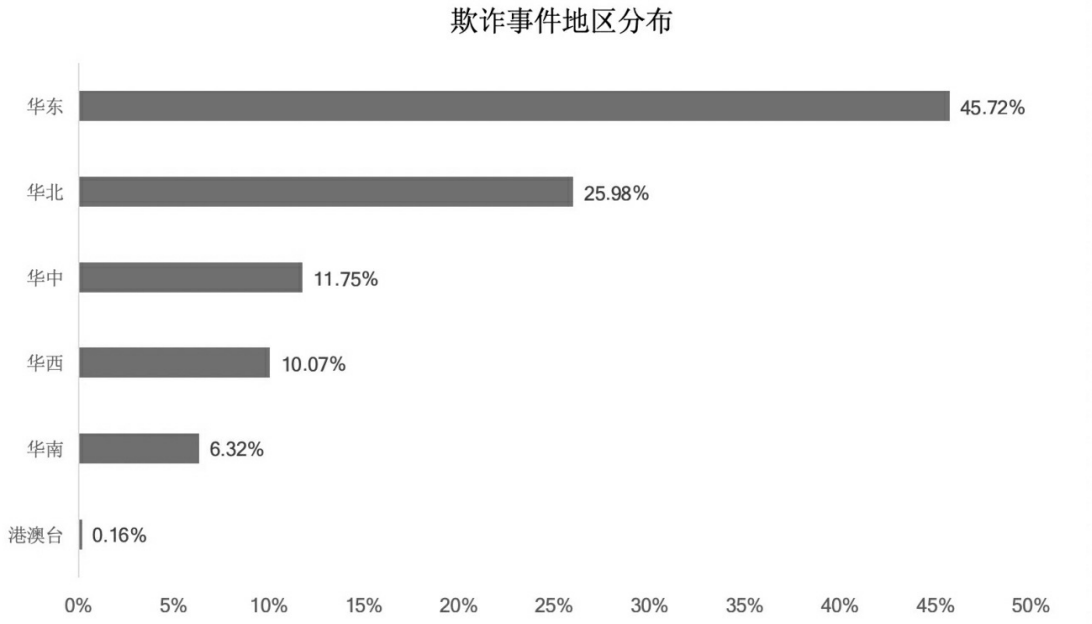

图1.6　欺诈攻击来源区域分布

通过对参与欺诈活动的IP 地址进行分析，发现近10%的欺诈行为都来自家用宽带IP 地址。

通过知识图谱关联分析，我们把使用相同手机号、设备的黑产进行聚合，可以对黑产团伙进行识别和深入挖掘。在这些关联数据中，聚集成簇的就被定义为“团伙”，团伙中出现的手机号和设备就可以被视为“成员”。我们累计发现并标记了超过8万人的“超大规模”团伙，涉及的手机号、设备节点数量总计超过10万个，其规模分布如图1.7所示。

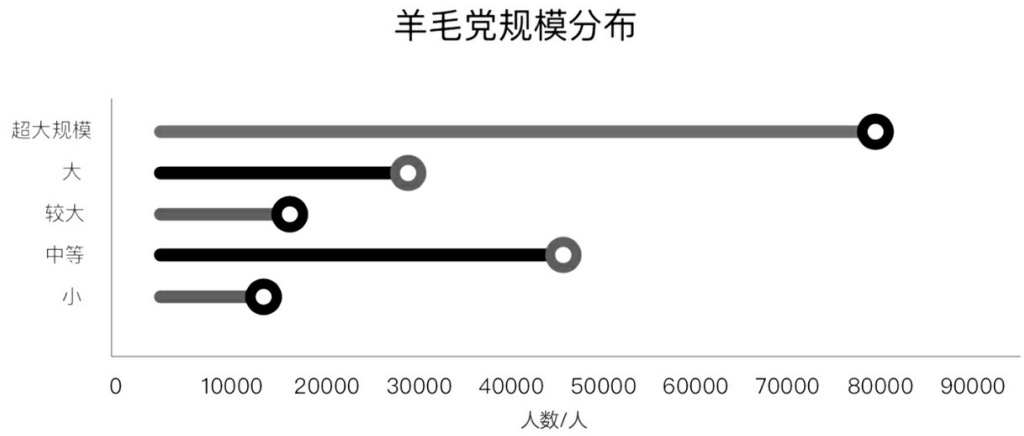

图1.7　羊毛党规模分布

1.5 电信欺诈黑产

在现实世界中还有一类更加凶残的黑产团伙——电信诈骗团伙。这类黑产团伙的危害远远超过上文所说的羊毛党类黑产。他们通常通过暗网等渠道购买大量公民隐私数据，通过分析后选定欺诈目标，编写特定的剧本实施诈骗。其剧本编写的针对性非常强，往往会击中目标受害用户的心理脆弱点，所以欺诈成功率非常高。我们曾多次协助银行客户进行电信诈骗案件的分析和对抗，持续追踪了一个藏匿在境外的大型电信诈骗团伙。该团伙冒充司法机关对大量境内网民进行定向诈骗，在3个月内成功欺诈了近7000人，诈骗金额高达近2亿元（见图1.8）。其洗钱的渠道和网络赌博团伙类似，往往会经过“水房”（在行业里指专业的洗钱渠道）出境。

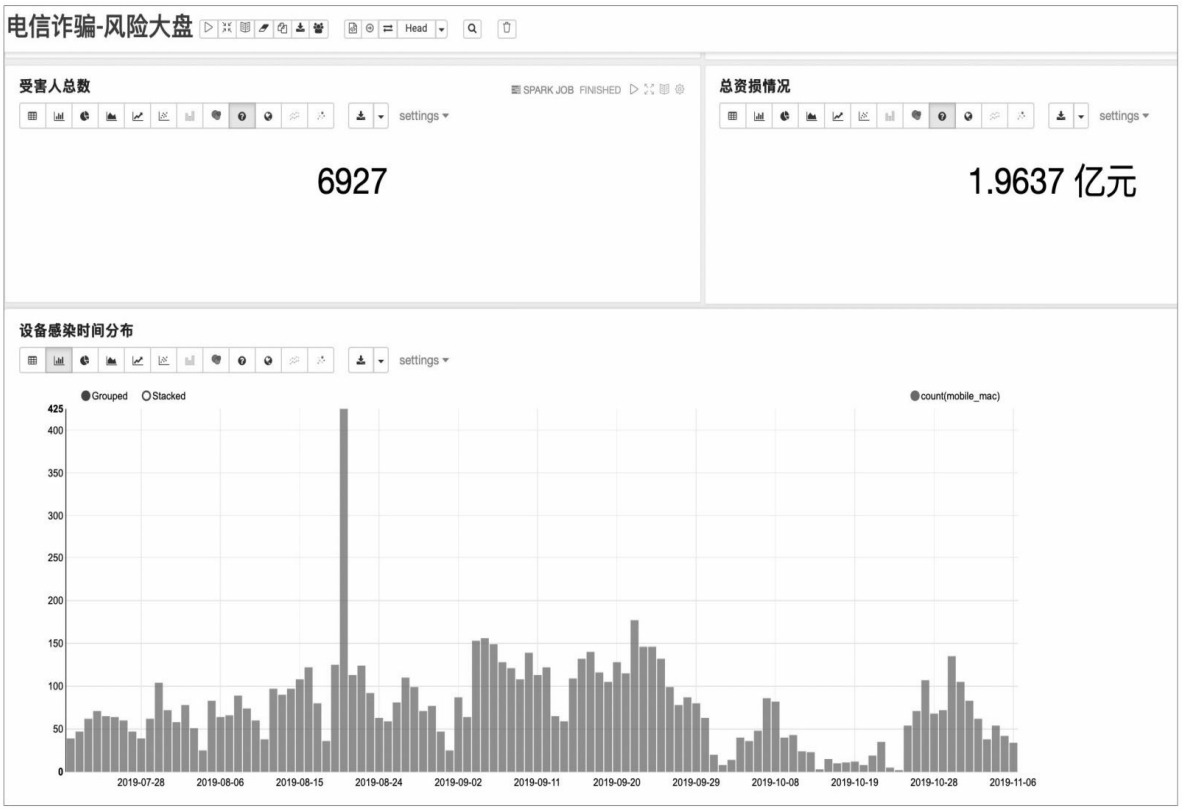

图1.8　电信诈骗案件追踪

1.6 本章小结

本章主要介绍了黑色产业链发展的态势、规模和运作的体系。所谓“知己知彼，百战不殆”，在对抗黑产之前，必须先对他们进行充分的了解。

黑色产业链之所以难以斩断，除技术因素之外，还和它形成的利益生态有极大的关系。当黑产团伙规模发展到一定程度后，它就成了一种能够干扰互联网正常生态的力量。

不少看似正规的互联网企业为了获得极速的成长，甚至会主动引入黑产生态的流量。