同盾科技
www.tongdun.cn

智能网络·诚信互联

2020
反欺诈年度报告

2020 Anti-fraud Annual Report

出品方

XIAODUN
小盾安全

2021年01月

2020 反欺诈年度报告

2020 Anti-fraud Annual Report

2020年伊始，新冠肺炎疫情“黑天鹅事件”的发生，对各行各业产生了严重影响。一方面餐饮、旅游、娱乐等服务消费行业的正常生产经营活动停摆，造成了巨大经济损失；另一方面中小微企业遭到供需“两端冲击”，资金链处于断裂边缘，面临生死考验。一场突如其来的疫情搅动着国际局势也考验着国计民生，物理距离的隔离推动着整个社会资源、生活习惯向线上更快的迁移。面对疫情，企业将重新审视在不确定性环境下的数字化能力和快速应变能力，提升疫情过后的企业数字化免疫力和生存力，以提高其他不确定因素带来的挑战。通过智能化和自动化，提升效率和降低成本。“后疫情时期”，数字化转型正在成为技术、产业发展的新高地。

在疫情的推动下，金融业智能化、政企数字化加速转型更加提速；在线教育、线上办公、社区电商等行业井喷式发展；直播电商走进公众生活，GMV屡创新高。网络流量史无前例爆发的同时各种欺诈风险暗流涌动。本篇报告旨通过对2020年全年国内外近千个域名、数千亿次的网络请求分析，以黑产作案工具、流程为切入点，结合监管治理动态对2020年典型欺诈场景和案例深入剖析，进一步探究未来风险演变趋势，并提出数字化风险防控建议，在此次年度特刊中，我们希望与业界一同探讨未来行业可能出现的变革以及作为从业者如何从容应对挑战。

第一章
2020网络欺诈现状分析

一、总体概况

2020年的疫情改变了社会交互的模式，疫情驱动的数字化快速转型使得相伴而生的数字风险比预想中到来的更快更迅猛。

《2020年全球风险报告》由世界经济论坛携手Marsh & McLennan Companies联合发布，广泛深入的分析了2020年以及未来十年可能对世界产生影响的重大风险问题，按照发生可能性和影响力对风险进行了排序。根据《2020年全球风险报告》预测，数据欺诈和网络攻击的风险仅次于极端天气和自然灾害，已经成为全球需要共同面对的风险。

按**发生可能性**排列的前十大风险

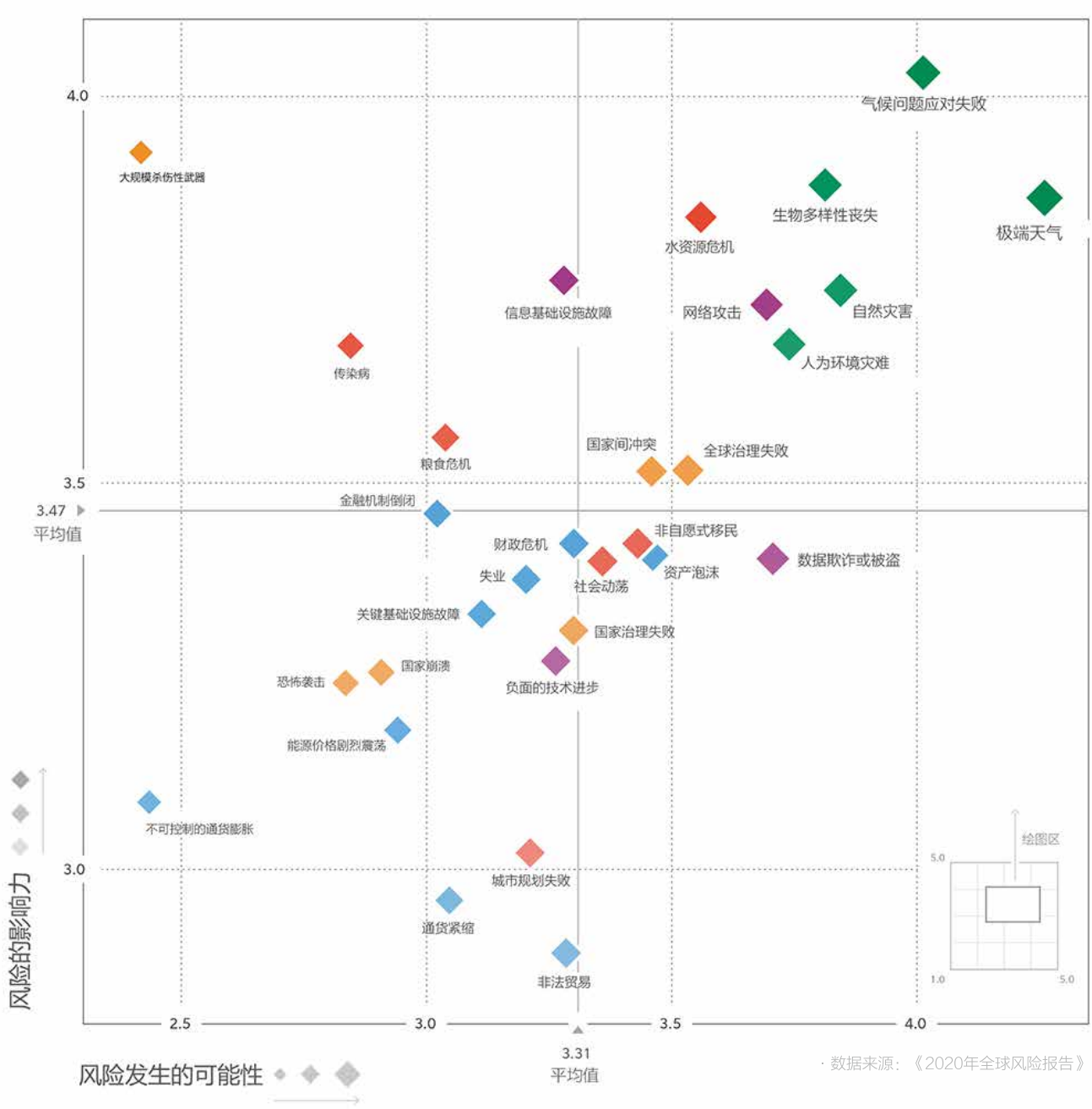
1. 极端天气
2. 气候问题应对失败
3. 自然灾害
4. 生物多样性丧失
5. 人为环境灾难
6. 数据欺诈或被窃
7. 网络攻击
8. 水资源危机
9. 全球治理失败
10. 资产泡沫

按**影响力**排列的前十大风险

1. 气候问题应对失败
2. 大规模杀伤性武器
3. 生物多样性丧失
4. 极端天气
5. 水资源危机
6. 信息基础设施故障
7. 自然灾害
8. 网络攻击
9. 人为环境灾难
10. 传染病

风险分类

- 经济
- 环境
- 地缘政治
- 社会
- 科技



在数字化转型的背景下，场景与科技的深度融合使服务更加数字化、虚拟化，线下业务加速向线上业务迁移，非接触式的网络欺诈日益严峻，欺诈风险成为企业数字化转型和线上业务发展的重大挑战，信息倒卖、盗卡盗刷、薅羊毛、信贷欺诈、电信诈骗每年为行业带来超千亿经济损失。行业风险从传统网络安全向各类业务安全快速转移，企业将要面临更多来自外部的欺诈和未知威胁。企业安全团队将不仅要满足IT安全的要求，还需要为业务安全运营提供有力的安全支撑，以应对全面数字化时代复杂多变的安全形势。

二、网络欺诈形式

网络欺诈形式多样，手段繁多，主要包括以下形式：

1、垃圾注册：黑产通过机器脚本批量化操作，注册大量账号，为后续营销活动薅羊毛、刷人气、广告导流等行为做准备，对企业后续业务环节埋下隐患的同时，由于平台内产生了大量虚假账号，会对用户留存率等统计指标造成严重干扰，甚至可能导致平台产品发展决策性失误。

2、恶意登录：包括拖库、撞库和暴力破解，即非法盗取并大批量尝试登录他人账号，最终导致平台信息泄露，造成用户经济，给平台带来信誉影响，尤其是电商、游戏、社交、支付等类型平台尤为常见。

3、虚假刷量：通过虚假刷量方式来提高曝光度，如直播电商刷直播间人数、刷粉丝数、刷点赞、刷商品成交量等。

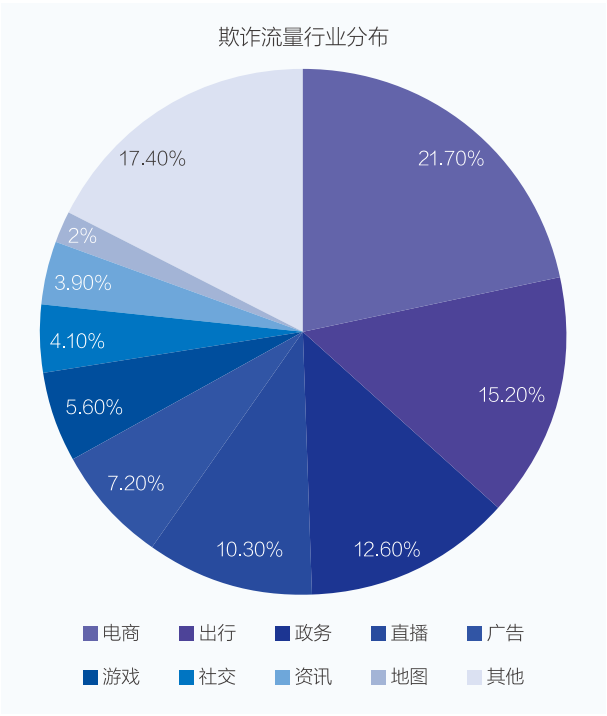
4、营销活动套利：滥用平台的各种营销活动机制，如新人奖励、用户裂变拉新奖励、签到奖励、秒杀优惠、商户补贴等，通过批量操作大量虚假账号参与平台营销活动，积少成多的方式进行套利。随着各平台风险监控力度的加强，黑产也在逐步改变欺诈方式，由原来的机器批量操作，改为人肉众包的形式，给企业识别欺诈分子带来了一定困扰。

5、交易欺诈：在交易支付环节，平台常会面临盗卡盗刷、恶意退款等风险，往往是企业提供了相应的产品或服务，却没有收到交易款项，造成直接经济损失。而且由于某些国外第三方支付机构并不能及时全面地通知企业欺诈情况，造成企业数据分析滞后，欺诈损失拦截不及时，风险较难控制。

以上列举了常见的黑产在互联网业务中的作案场景，而实际业务中，由于行业及业务属性的不同，欺诈分子利用平台技术或业务逻辑漏洞发起攻击的场景更是数不胜数。

三、网络欺诈分布

小盾安全根据全网情报统计，对欺诈行业分析、场景分布研究分析如下：



解读：

电商行业：一方面，受疫情隔离影响以及巨头电商平台对下沉用户群的覆盖力度增强，各大电商平台GMV屡创新高，各种营销活动层出不群（茅台秒杀、大额优惠券补贴、新手活动等），而与之伴随的是整个以欺诈流量为代表的完整黑灰产业链的枕戈待旦。另一方面，比价平台对于各家电商的持续价格爬虫流量也日益水涨船高。

出行行业：报告中的出行行业的主要欺诈流量集中在航司和OTA、二级代理商对于航司航班价格接口持续的查询，极大增加了航司的服务器压力，有可能导致航司查订比超过中航信规定标准，近而缴纳额外查询费用。2020年受疫情影响虽然整个出行行业欺诈流量同比去年有所下降，排名仍然高居第二。

政务网站：近年来越来越多的公司，利用国家公共平台的信息作为其商业化产品的重要数据来源（大数据征信产品，企业信息查询，车辆信息查询产品等），辅助以良好的交互体验、产品包装实现商业化的目的。这样大规模

的数据来源需要大量的机器爬虫来提升入库的效率，失信人员名单查询系统、中国裁判文书网、失信被执行人查询、中国及多国专利审查信息查询、商标查询、车辆违章信息查询系统、国家企业信用信息公示系统、全国组织机构代码管理中心等网站为重灾区。

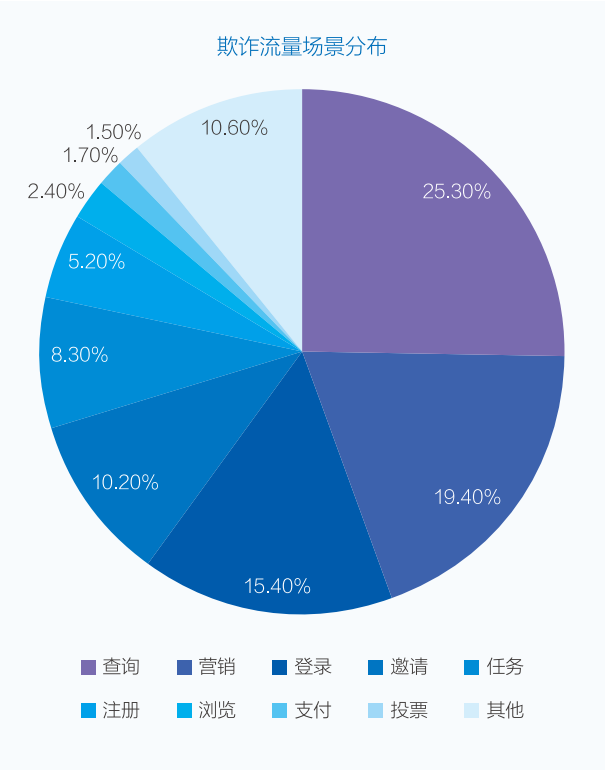
直播行业：除了传统秀场和游戏直播的主流平台外，2020年电商直播的持续发酵吸引了更多的流量，以抖音、快手为代表的短视频平台与传统电商形成分庭抗礼之势，欺诈流量在直播行业绝大部分流向虚假人气、点赞关注的场景。

广告行业：虚假流量往往伴随着企业主和广告渠道的结算方式，不论是应用商店的下载，还是信息流广告CPA\CPC\CPM的结算方式，都有大量虚假流量的注入来骗取企业主的投放费用。

游戏行业：由于疫情的原因，2020年游戏行业也迎来了流量的爆发，同时更多的欺诈行为也充斥其中，主要体现在渠道下载刷量、外挂以及模拟器挂机、恶意退款等。

社交行业：作为用户交互最频繁的行业，账户是社交最重要的一环，欺诈流量也是围绕批量注册、养号以及垃圾广告等场景，洗钱套现、恶意退款在社交行业也同样存在。

资讯行业：主要集中在门户新闻网站内容爬虫、网赚平台的虚假流量。



解读：

场景依托于行业、是线上利益具像化的呈现方式，也是企业方和灰黑产对抗的风暴中心，绝大多数企业通过线上策略规则、模型实现对欺诈行为的实时判断与处置。

· 查询，尤其是非登录状态下的查询作为线上资源获取的最重要环节，欺诈流量占比超过1/4。

· 营销活动是重灾区，黑产滥用平台的各种营销活动机制，如新人奖励、用户裂变拉新奖励、签到奖励、秒杀优惠、商户补贴等，通过批量操作大量虚假账号积少成多的方式进行套利。电商平台的“百亿补贴”给黑产从业者带来了极大的利好，一部分营销补贴流进黑产手中，从裂变拉新-注册登录-营销活动（抢购、投票、浏览...）-交易支付，欺诈场景贯穿这个业务流程，欺诈流量同样趋之若鹜。

四、黑产欺诈环节

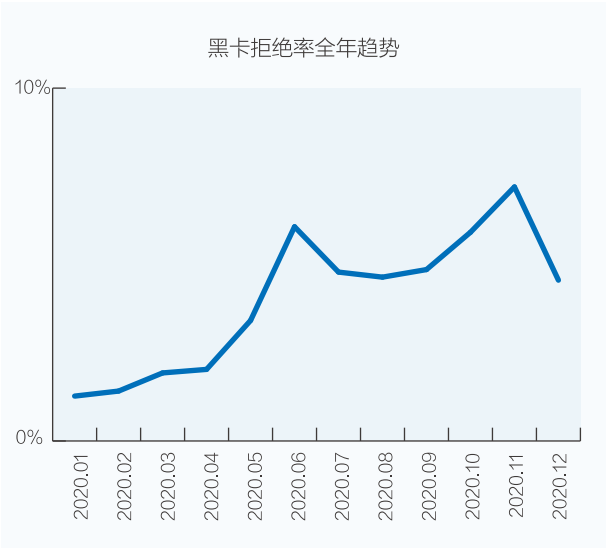
黑产作案流程

上游	资源类		工具类		
	账户/密码	设备信息	接码平台	打码平台	
	手机号码	身份信息	众包网站	情报工具	
	邮箱	企业资质	群控/云控系统设备		
	IP		定制化软件		
欺诈行为	网络诈骗	广告刷量	虚假人气	薅羊毛	数据爬取
	电信诈骗	恶意注册	刷量刷票	游戏外挂	机刷广告
下游	产品转卖	渠道分成	收费服务	博彩引流	
	账号贩卖	数据变现	恶意退款	教程传播	

随着整体技术水平的发展进步，大量的物联网卡、虚拟专用服务器（VPS，Virtual Private Server）秒拨更换IP、云手机、iOS模拟器等资源和工具为黑产提供了巨大的便利，从而更高效且隐蔽地发起各式攻击。目前黑产从上游资源、工具类获取，中游欺诈行为的产生，下游资源变现都有非常成熟的产业链条，且分工明确，专业度较高。

主要工具

1、虚拟手机号

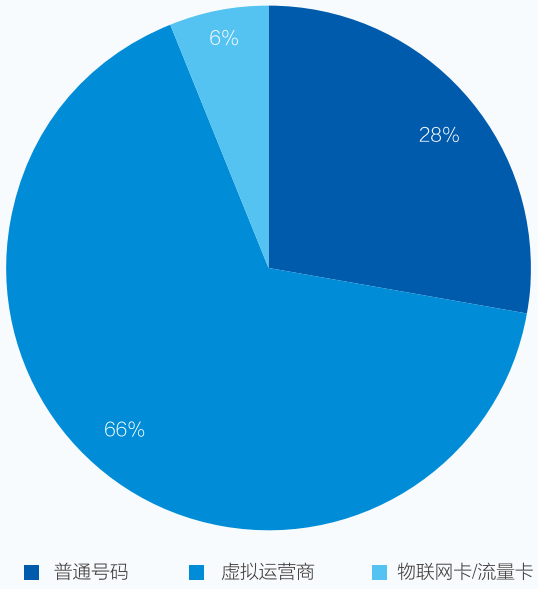


解读：

纵观全年趋势，从5月下旬开始随着年中大促拉开帷幕，交易拒绝量开始逐步上升，在6月和11月由于营销活动遭受黑产攻击，交易拒绝率相较上月显著上升，和每年整个电商行业两次最大的“购物节”流量趋势基本契合，营销活动不仅是消费者的“狂欢”，同样也是黑灰产的“盛宴”。

2020年10月10日，国务院打击治理电信网络新型违法犯罪工作部际联席会议部署开展以打击、治理、惩戒开办及贩卖“两卡”（手机卡、银行卡）违法犯罪团伙为主要内容的“断卡”行动以来卡商存量已经急剧下降，明年2季度市面上黑卡数量应该会有明显下降趋势体现。

黑名单号码类型分布



解读：

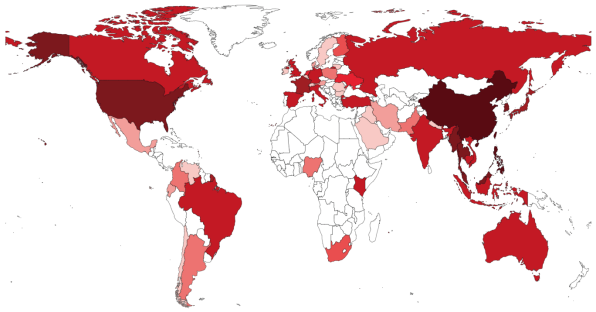
在整个黑卡类型分布中，虚拟运营商虽然目前开放的号段不多，贡献却超过60%，原因有两点：

· 虽然是三大运营商下发号段，但是销售管理属于虚拟运营商自己把控，入网门槛相对较低，给了黑产可乘之机。

· 真实用户占比逐年上升，业务方无法根据号段直接设置风控规则。

2、IP

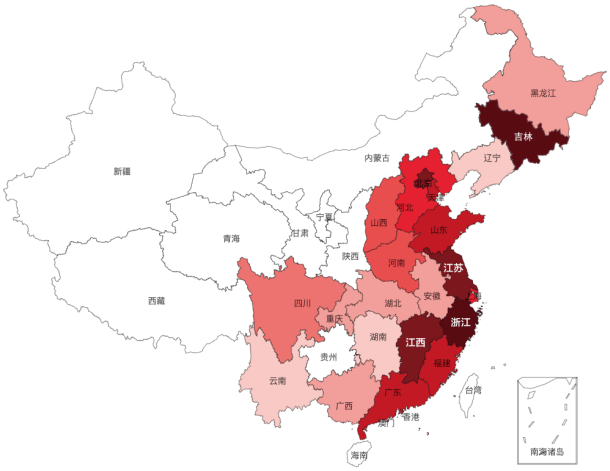
全球机器流量分布



解读：

当前全球机器流量分布，亚洲占比超50%，其次为美国为代表的北美洲以及欧洲地区。

机器流量当前在国内的分布



解读：

机器流量当前在国内的分布，并未出现在传统的北上广深等互联网发展较快的区域。吉林、江西、福建、山东等地区甚至超越上海，进入前十。而吉林省，更是超越北京，占据全国机器流量分布榜单次席。

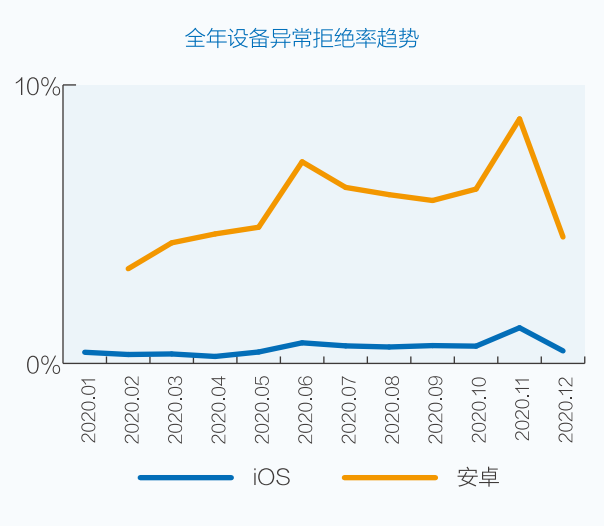
IPv6逐渐开始被黑产利用

随着全球IPv6的逐步普及，在整个2020年有近于8%的攻击来源为IPv6地址，黑产对于IPv6的使用，势必在未来的1-2年内将攻防态势拉到一个新的高度，因为这意味着：

· 黑产将拥有比起IPv4来说取之不尽的资源池。

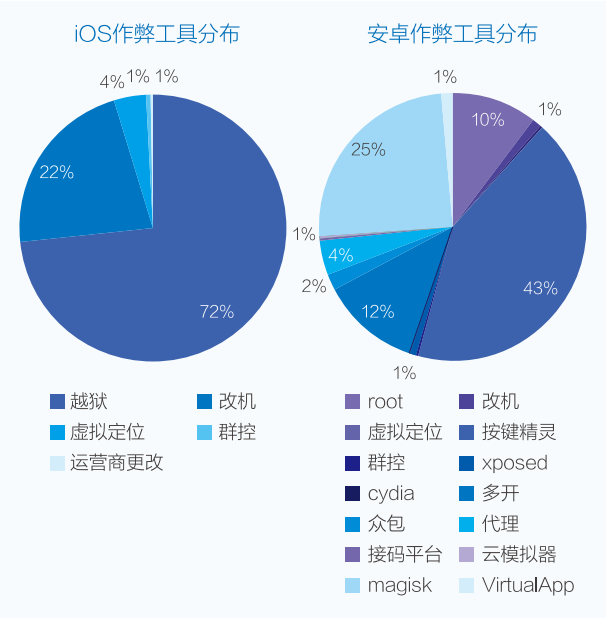
· 行业多年积累的风险库以及丰富的标签将逐渐失去作用，各平台需要重新构造。

3、设备画像



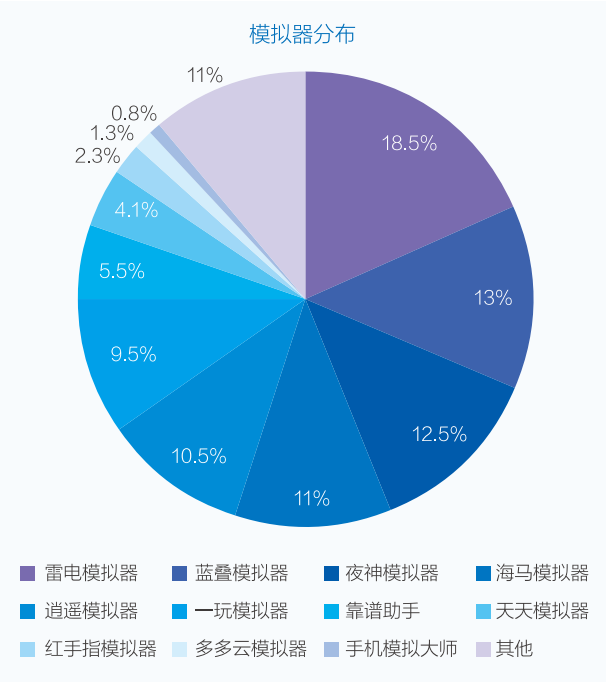
解读：

由于底层生态安全系统和价格因素的不同，且基于Android的开源特点，作弊工具的开发和刷机技术难度低，大部分黑产采用Android设备进行作弊，安卓设备不论从黑产保有量还是活跃度都远超于iOS设备，其中安卓系统端，OPPO和华为机型使用次数较高。整体趋势从5月上旬开始，在设备端的攻击趋势还是持续陡增，一直持续到11月末，每年12月-次年4月为整个黑产相对意义上蛰伏期。



解读：

iOS设备因为其本身更加封闭的系统，所以安全性相比安卓设备更加良好，对应的破解方法也屈指可数，安卓设备的破解工具则是五花八门。



解读：

市面上针对安卓设备的模拟器有上百款，一般有专业技术人员维护，更新速度快、性能稳定，是黑产提高效率、规模化作业的不二选择。

第二章
欺诈行业热点

2020年，全国公安机关网安部门发起“净网2020”打击网络黑产犯罪集群战役，重拳打击为电信网络诈骗、网络赌博、网络水军等突出违法犯罪提供网号恶意注册、技术支撑、支付结算、推广引流等服务的违法犯罪活动，共侦办刑事案件4453起，抓获违法犯罪嫌疑人14311名（含电信运营商内部工作人员152名），查处关停网络接码平台38个，捣毁“猫池”窝点60个，查获、关停涉案网络账号2.2亿余个。据相关数据显示，网络活跃接码平台日接码量降幅67%，黑市手机号数量降幅近50%，有力维护了网络秩序。

一、电信网络诈骗

1、电信网络诈骗定义

电信网络新型违法犯罪（也叫“电信诈骗”）是指不法分子通过电话、网络和短信方式，编造虚假信息，设置骗局，对受害人实施远程、非接触式诈骗，诱使受害人打款或转账的犯罪行为。

电信诈骗的四个主要环节包括：

（1）精准信息获取：诈骗分子通过非法窃取或购买社会上泄漏的个人信息，包括身份证信息、手机号码、银行卡号和密码等。个人信息泄漏事精准诈骗的根源。

（2）诈骗脚本设计：诈骗分子模拟真实场景设计各种诈骗脚本，如近期高发的兼职刷单、冒充网购客服等。

（3）通讯联络诱导：诈骗分子利用设计的脚本和之前获取的个人信息，通过电话、短信、互联网等渠道联络受害人，骗取受害人信任进而实施诈骗。

（4）资金支付转移：诈骗分子诱导受害人通过网上支付等方式向其指定账户转款，并转移受害人资金。

2、监管政策形式

为防范治理新型电信网络诈骗，世界主要国家和地区开展推进打击防范治理工作，国际主要国家和地区治理内容包括：

· 深化个人信息保护制度：目前全球已有126个国家制定了专门针对个人信息保护的法律，加大违法行为惩罚力度。

· 强化技术手段提升诈骗识别能力：美国国防部和微软、麻省理工学院等高校积极开展新型诈骗防范技术研发。

· 加大诈骗全流程监控：2019年2月，英国政府联合银行业界，发布了《授权推送付款（APP）诈骗自律守则》。

· 加强警示教育提升民众防范意识：2018年，以色列国家网络管理局（INCD）发布“新型网络攻击”警告。

为有效遏制新型电信网络诈骗产生蔓延，我国积极开展治理措施包括，制定出台相关制度，逐步完善监管体系，要求建立健全技术手段，政府联合企业加强防控技术研发，诈骗治理联防联控，通过分析诈骗特征，提升诈骗识别、预警、拦截和处置能力，打击黑产团伙和链条，具体要求包括：

· 2018年工信部印发《关于纵深推进防范打击通讯信息诈骗工作的通知》，针对电信网络诈骗治理工作遇到的新情况新问题，明确了九项重点任务，包括切实加强实人认证工作、依法开展网上诈骗信息治理等。

· 2019年工信部发布《工业和信息化部办公厅关于进一步做好 2019 年防范治理电信网络诈骗重点工作的通知》(工信厅网安函〔2019〕108 号文)。

· 2019年中国人民银行发布《中国人民银行关于进一步加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》（银发85号文）。

· 2020年公安部发布《关于新冠肺炎疫情期间依法严厉打击跨境赌博和电信网络诈骗的通告》，个人信息保护与实名登记成为当前监管治理工作重点，强化通报约谈和责任落实。

3、典型案例及治理成效

在低成本、高效益的巨大诱惑下，诈骗分子不断翻新手法、迭代技术、细化分工，更加隐蔽化和智能化地实施诈骗犯罪。近期新型网络诈骗方式主要有以下几种：

“杀鱼盘”主要指以“金融服务”为理由的诈骗，常见有提额、贷款，受害人被诈骗分子称为“鱼”。诈骗分子称可以提高贷款额度吸引人联络，在用虚假链接诱骗受害者付款，骗取钱财。“杀鸟盘”主要又称兼职/刷单诈骗，诈骗分子发布高薪兼职信息吸引受害人参与，设下套路不断鼓动受害者投钱代刷，最终骗取钱财。在整个诈骗过程中，使用“小诱饵”方式获取受害人信任。“杀猪盘”主要指情感诈骗，受害人被诈骗分子称为“猪”。诈骗分子通过婚恋平台、社交软件等方式在网上筛选单身人群，通过聊天发展情感取得信任，诱骗受害人参与网络赌博或其他投资，骗取钱财。近年来因不断出现P2P暴雷，诈骗分子紧跟形式，又编撰出了帮助受害人要账等诈骗脚本。

当前，全国电信网络诈骗犯罪形势严峻复杂，非法开办贩卖电话卡、银行卡是此类犯罪持续高发的重要根源，危害十分严重。为严厉打击整治涉“两卡”违法犯罪活动，坚决遏制电信网络诈骗犯罪高发态势。2020年10月10日，国务院打击治理电信网络新型违法犯罪工作部际联席会议全国“断卡”行动部署会召开。断卡包括：

· 手机卡：

包括平时所用的三大运营商的手机卡、虚拟运营商的电话卡和物联网卡。

· 银行卡：

包括个人银行卡、对公账户、结算卡、非银行支付机构账户，即我们平时所说的微信、支付宝等第三方支付。

任何一宗电信网络诈骗，都离不开信息流（通过电话、短信、网络等方式对被害人进行洗脑）和资金流（通过银行卡、第三方支付等转账）两个要素，而信息流和资金流最重要的载体就是手机卡和银行卡。

2020年以来，按照全国打击治理电信网络新型违法犯罪工作电视电话会议部署要求，各地各部门深入开展打击治理工作，全国共破获电信网络诈骗案件15.5万起，抓获嫌疑人14.5万名，同比分别上升65.6%和74.1%；累计封堵涉诈域名网址21万个，拦截处置诈骗电话5100万余次、诈骗短信6.3亿余条，成功止付冻结涉案资金1000余亿元。

二、网络赌博

1、网络赌博定义

网络赌博，通常指利用互联网，以钱财为赌注，使用某种方式或者工具比输赢来非法获取钱财的博彩行为。网络博彩类型繁多，由于受时间、地点等不确定因素影响，一般还是以“结果”型的赌法为主（例如赌球、赌马、骰宝、轮盘、网上百家乐等）。网络赌博是违法犯罪行为，具欺骗性和危害性，“庄赢客输”“十赌十输”是赌场的“不变规律”。

2、监管政策形势

公安部治安管理局局长李京生于2020年初在京召开新闻发布会，重点介绍了2019年全国公安机关开展打击整治跨境网络赌博犯罪情况和典型案件。通报介绍2019年以来，公安部共督办各地公安机关侦破网络赌博刑事案件7200余起，抓获犯罪嫌疑人2.5万名，查扣冻结涉赌资金逾180亿元，打掉非法地下钱庄、网络支付等团伙300余个。

· 2020年4月，公安部发布《关于新冠肺炎疫情期间依法严厉打击跨境赌博和电信网络诈骗犯罪的通告》，公安机关将协同有关部门，加强对跨境赌博和电信网络诈骗的综合治理，加大非法资金管控力度，严肃查处一批违法违规为跨境赌资提供结算服务的支付机构，最大限度阻断资金非法流通。对相关违法犯罪人员，还将在出入境管理、个人征信等方面加大管控惩戒力度，建立参赌及从业人员“黑名单”等制度。

· 2020年5月，中国人民银行发布《打击治理跨境赌博金融监管工作组关于印发<涉赌涉诈可疑资金特征及账户线索核查要点>的通知》（银支付49号文），央行要求各银行、支付机构、清算机构要参考《核查要点》，对已有风险防控措施进行查漏补缺，完善关于客户、账户的尽职调查措施，配备充足人员，开发和运用有效金融科技和大数据系统，健全关于本网络处理的跨机构资金交易风险监测识别、预警、处理机制，实现对赌博和电信诈骗“资金链”有效治理。

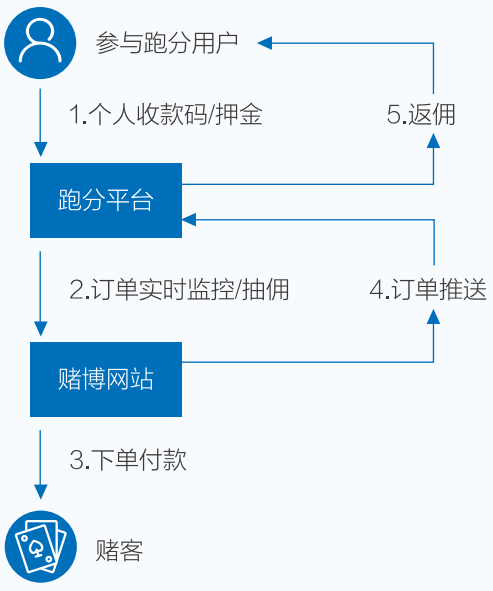
监管各部门要求始终保持严打高压态势，强化主动打击、规模打击、依法打击，针对周边重点涉赌国家、国际赌博集团，深度挖掘重大线索，集中攻坚一批重大跨境网络赌博案件，强化彩票、网络游戏、对外投资和劳务合作等重点行业监管措施，推动形成防控治理工作新机制新格局。

3.典型案例及治理成效

2019年开始，支付行业进入大整治。随着净网行动的严厉打击，涉及黑灰产的支付通道被一一封堵，部分黑灰产的不法资金难以通过原来的支付通道流出，业内人士称之为“最强清理”。于是，一条名为“跑分”的产业链全面兴起，目前产业链已有逾十万人参与，三大参与方包括用户、代理和跑分平台。

通过开发“跑分”网络平台，吸纳会员，形成“码农—码商—代理—平台—支付通道—盘口”资金流转闭环路径，利用“第四方支付”为境外赌博网站等非法商户提供资金支付通道，以赚取佣金获利。据不完全统计，跑分链条产品已为黑灰产和赌博洗钱提供了上百亿的资金。这条新的黑色支付链条正在慢慢成长壮大，一条支付暗道已经形成。

典型赌博网站跑分流程图



今年4月，惠州市公安局网警支队接线索通报，惠州本地有网民在互联网上大肆推广某支付平台和招收代理兼职的广告信息。宣传只需向平台缴纳一定金额的保证金并

上传收款账户，就可以足不出户获取高额返佣和提成。惠州网警根据掌握的线索进行初步分析，发现该平台的运营人员通过招收代理和组建工作室的方式，利用会员的收款账户为境外网络赌博网站以及金融投资诈骗平台提供接收、流转、洗白资金服务，并且通过境外聊天软件以逃避警方打击，具有极强的反侦察意识。

获悉此线索后，惠州市公安局迅速成立专案组开展案件侦查，办案民警利用智慧新警务手段，摸清了一条由“技术开发商—推广运营商—跑分参与者”组成的网络黑产链条。

一是“技术开发商”违反国家支付结算制度，在互联网上非法搭建“第四方支付”管理后台，采用“USDT”货币的方式进行结算，为境外赌博网站等平台提供支付通道服务。

二是“推广运营商”通过网络工具收集互联网上涉及网络黑支付需求的论坛、贴吧、QQ群组等网络平台，再以群发广告的方式，寻找有非法资金结算需求的境外网络赌博、诈骗等犯罪团伙，同时在互联网上发布广告以高额返佣吸收众多兼职人员成为“跑分”人员。

三是“跑分”人员在向平台缴纳一定金额的保证金后，就可以在平台上“抢单”。接单后，平台直接扣除“跑分”人员之前所购买的等额保证金，并将相应的USDT充值码提供给赌客，赌客通过支付宝、银行卡充值等额的USDT币至“跑分”人员的账户。

四是平台根据流水返还佣金给跑分人员。因此，众多“跑分”人员间接参与到洗白赌资的环节中，为犯罪分子提供帮助。经查，全国各地“跑分”人员多达3000余人。

6月8日，在广东省公安厅的统一指挥下，惠州警方在深圳龙岗、惠州惠城、博罗等地同时开展收网行动，打掉了一个利用USDT数字货币经营第四方支付平台的犯罪团伙，共抓获涉案犯罪嫌疑人76名，查处涉案网络支付工作室4家，捣毁网络赌博团伙2个。经初步核实，该平台运营近15个月，为境外120个赌博网站以及70家投资诈骗平台提供资金结算服务，涉案金额达1.2亿元。该案是全国侦破的首例利用USDT数字货币为违法犯罪活动提供网络支付服务的案件。

三、直播电商刷量

1、直播电商刷量定义

直播电商指让商家和网红（KOL）通过流媒体的形式对其粉丝和消费者进行营销推广，以内容连接用户，通过主播推荐、产品展示与消费场景，激发消费者的潜在购买需求。直播带货的刷数据主要分为两种：刷人气和刷销量。

· 刷人气：主要是为了制造热闹，增加观众停留时长，因为观看人数是实时更新的数据，直播间的任何人都能看到，高人气的直播间转化率会明显比低人气的直播间要高，制造热闹假象。

· 刷销量：直播刷销量本质上跟电商卖家刷单没有什么区别，直播结束后的成交量往往预示着主播带货能力，想要获得更多商业资源，刷量是一种重要的手段。

2、监管政策形势

2020年是直播电商爆发的一年，随着直播电商的火热，数据造假、夸大宣传问题层出不穷，也因此迎来了监管。越来越多的主播利用黑产渠道进行刷量，平台的监管也随之越来越严格：

· 6月24日，中国广告协会发布国内首份《网络直播营销行为规范》（以下简称规范），对直播电商中的各类角色、行为都作了全面的定义和规范；

· 11月5日，国家市场监管总局发布《关于加强网络直播营销活动监管的指导意见》，明确直播禁止发布的内容和依法查处的8类违法行为；

· 11月13日，国家网信办就《互联网直播营销信息内容服务管理规定（征求意见稿）》向社会公开征求意见，明令禁止主播发布虚假信息，欺骗、误导用户；

· 11月23日，国家广播电视总局发布《关于加强网络秀场直播和电商直播管理的通知》，强调对于多次出现问

题的直播间和主播，平台应采取停止推荐、限制时长、排序沉底、限期整改等处理措施，对于问题性质严重、屡教不改的，关闭直播间，将相关主播纳入黑名单并向广播电视主管部门报告，不允许其更换“马甲”或更换平台后再度开播。

监管政策传递出直播带货急需合规化的明确信息，对直播电商数据造假、产品问题、虚假宣传等问题进行界定和规范，引导直播电商健康、有序发展。

3、典型案例及治理成效

11月11日晚，某脱口秀演员被邀嘉宾在某平台参与了一场主要销售数码产品的带货直播，前端显示为311万观看。而一位全程参与此次直播的工作人员表示，当天结束时的311万观众中，只有不到11万真实存在，其他观众人数都是花钱刷量，而评论区与脱口秀演员亲切互动的“粉丝”的评论，绝大部分是机刷。

基于对10月20日—11月15日期间相关消费维权情况的网络大数据舆情分析，中国消费者协会在微信公众号发布《“双11”消费维权舆情分析报告》（以下简称“《报告》”）。《报告》指出，“监测期内，共收集有关‘直播带货’类负面信息334083条。每日负面信息量较为平稳，日均在12373条左右，其中11月11日舆情信息量最高。”从本次监测的舆情反馈来看，直播带货的“槽点”主要集中在明星带货涉嫌刷单造假，售后服务满意度低、体验较差两个方面。《报告》认为，一方面，观看人数吹牛、销售数据“注水”等“影响力”指标的造假，已经形成一条产业链。而另一方面，恶意刷单、花式踢馆、虚假举报等同业竞争也污染了直播生态。

四、营销活动套利

1、营销活动套利定义

营销活动套利，也被称为“薅羊毛”，在风控领域，对薅羊毛用户的定义比较多样化，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和价值的用户。还有一些用户把薅羊毛当做职业，利用商家、平台、运营商的漏洞，来大量攫取利益，甚至进行诈骗，对企业造成的损失以及带来的社会问题更加严重。几经演变，部分“薅羊毛”行为逐渐拥有了分工明确的产业链条，成为游走在法律空白地带的黑灰产业，与违法犯罪扯上关系。许多不法分子借助互联网平台推出的众多优惠活动进行恶意的资源套取和倒卖以达到获利的目的，并导致这些优惠无法流入营销目标用户手中，对互联网平台以及用户都造成了巨大的损失。

2、监管政策形式

受疫情影响，为提振国内经济，很多地区都采取消费券补贴方式促消费回暖。但据新华社报道，伴随抢券热潮，目前，“羊毛党”利用一些技术手段可以实现囤券：有人写程序、开外挂抢券；有人通过虚拟IP地址或虚拟定位，绕开消费券领取的地域限制，在全国范围内组团抢。所以往往是“羊毛党”大量囤券，而普通市民一券难求。在此情况下，多部门联手，加大对恶意“薅羊毛”行为的打击力度，以全流程监管遏止消费券套现交易行为已成当务之急。

“羊毛党”虚假交易套取消费券可能构成诈骗罪。商家如果专门通过帮市民套现来获利，且数额较大的，同样可能涉嫌诈骗犯罪。“薅羊毛”行为可能面临刑事风险，构成诈骗罪、侵犯公民个人信息罪和计算机系统犯罪。

（1）诈骗罪

《刑法》第二百六十六条规定：“诈骗公私财物，数额较大的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金；数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。本法另有规定的，依照规定。”“薅羊毛”行为如果利用了平台的处罚规则，恶意“薅羊毛”之后以恶意投诉或者举报等行为获取保证金或者赔偿金的行为如果达到数额较大的标准则涉嫌构成诈骗罪。施害者是“薅羊毛”者，受害者是店铺，受骗者及有权处分者是电商平台，形成三角诈骗的模式。

（2）侵犯公民个人信息罪

《刑法》第二百五十三条之一：“违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。”一般业务方防止“薅羊毛”行为，店铺在促销活动时会对账号采取限制，而黑产通过购买大量账号来“薅羊毛”。这些账号包含有公民的真实姓名、联系方式、身份证号等信息，如果达到情节严重，则构成侵犯公民个人信息罪。

（3）计算机系统犯罪

“薅羊毛”行为还可能触犯第二百八十五条第二款【非法获取计算机信息系统数据、非法控制计算机信息系统罪】和第二百八十六条【破坏计算机信息系统罪】。如果“薅羊毛”行为是通过非法获取计算机信息系统数据、非法控制计算机信息系统罪或者破坏计算机信息系统等手段进行的，那么还可能涉及计算机系统犯罪。

3、典型案例及治理成效

案例1：延误险薅羊毛

2020年6月9日，南京市公安局发布消息称，鼓楼警方成功侦破一起涉嫌航班延误保险诈骗案。从2015年至案发，曾有过航空服务类工作经历的李某，为获得延误险索赔，会在网络上挑选延误率较高的航班，并使用亲朋好友的20多个身份证号以及护照号购买机票，每一个身份最多购买30-40份延误险，

警方介绍，购买一份延误保险的保费大概是40元左右，保险公司因飞机延误而赔付的金额为400到2000元不等。如果延误时间长，赔付费用甚至可以达到7000-8000多元。

李某称，其不会去乘坐这些航班，因此她时刻关注航班动态，如果了解到航班可能不会延误，她就会在飞机起飞之前把票退掉，尽量减少损失。一旦航班出现延误，李某便开始着手向保险公司索赔。

经初步统计，从2015年至案发，李某共实施诈骗近900次，获得理赔金近300万元。4月29日，南京警方将犯罪嫌疑人李某抓获归案，并依法对其采取刑事强制措施。

案例2：百万手机木马植入案件

浙江绍兴警方打掉一条“薅羊毛”黑色产业链，破获一起涉及31个省份、570万多部手机的非法控制计算机案。2020年4月8日从绍兴新昌县公安局获悉，吴某等20多位涉案嫌疑人已被提起公诉。

为招揽客户，一些电商平台会向新注册用户发优惠券、红包，网上有人专门搜集优惠券、红包，被称为“薅羊毛”。去年8月，新昌县居民小朱在用外婆的手机注册用户时发现无法收到验证码，怀疑手机被控制，向警方报案。新昌县网警测试发现，这部手机无法收到验证码、密码之类的短信，但其余短信能收发。警方进一步围绕涉案手机销售渠道展开调查，询问购买同款手机的37人，勘验手机25部，发现其中15部的短信收发不正常。经检测，这些手机的主板被植入木马程序，能把特定的短信上传指定服务器。

绍兴、新昌两级公安成立的专案组发现，接收回传短信的是深圳的一个手机号码，犯罪嫌疑人吴某和卢某随即进入警方视线，并确认犯罪团伙在深圳南山区一园区内办公，抓捕了相关嫌疑人，起获大量后台服务器数据及与上下游的交易合同。

经查，该团伙以犯罪嫌疑人吴某为首，制作可控制手机、识别拦截短信的木马程序，并与主板生产商合作，将木马程序植入到手机主板。

被植入木马程序激活的手机有500多万台，涉及功能机型号4500多种，受害者遍布31个省份。该团伙制作的木马主要针对老年人、小孩使用的老年机、儿童电话手表等功能机，因为这两类人相对不太关注短信验证类信息。之前，该团伙曾针对智能机种植木马，但用户很快会因收不到短信投诉，于是终止了对智能机的植入。

据介绍，该在团伙中，犯罪嫌疑人吴某专门负责木马病毒和对码平台搭建。犯罪嫌疑人邓某是一家手机主板生产厂家的技术负责人，他们把吴某提供的木马病毒嵌入手机主板，销售给手机生产商。吴某团伙利用木马程序获取的手机号、验证码，再通过在电商平台注册获取优惠券或红包，出售给网上的搜集者，形成黑色产业链。

第三章
欺诈行业趋势分析

一、产业背景

2020年9月16日，中国信通院发布《中国网络安全产业白皮书（2020年）》（简称《白皮书》）指出，我国网络安全产业规模呈现持续高速增长态势，预计2020年我国网络安全产业规模约为1702亿元，增速约为8.85%。

《白皮书》指出，我国网络安全产业规模呈现持续高速增长态势。2019年我国网络安全产业规模达到1563.59亿元，同比增长17.1%，预计2020年产业规模约为1702亿元，增速约为8.85%。随着网络安全行业的迅猛发展，现有网络安全产品和服务基本从传统网络安全领域延伸到了云、大数据、物联网、工业控制、5G和移动互联网等不同的应用场景。基于安全产品和服务的应用场景、保护对象和安全能力，我国网络安全产品和服务已覆盖基础安全、基础技术、安全系统、安全服务等多个维度，网络安全产品体系日益完备，产业活力日益增强。

二、风险演变趋势

1、诈骗手法升级演变，欺诈风险持续暴露

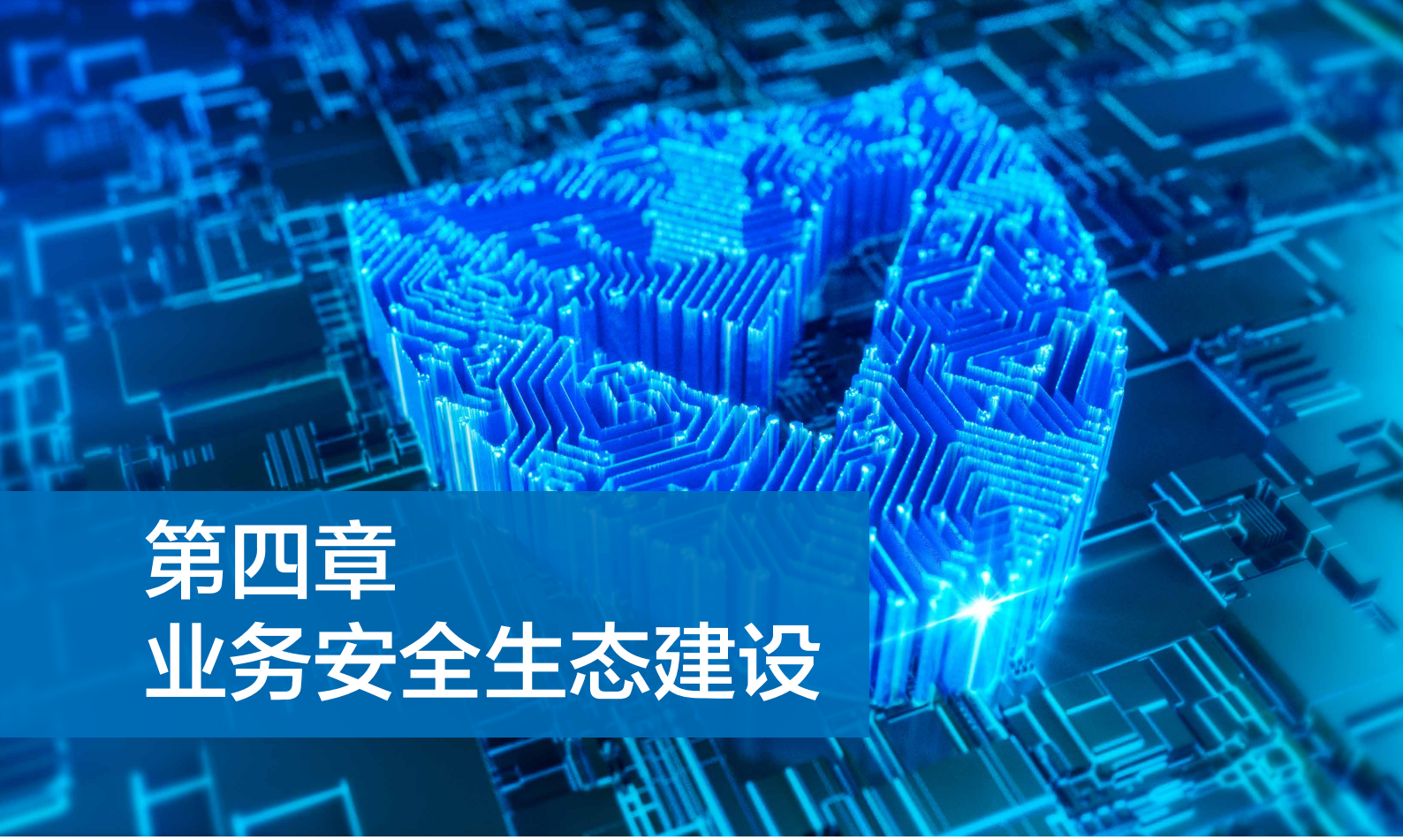
自去年以来，“杀猪盘”等为代表的新型电信诈骗发展迅猛，违法犯罪分子多从非法违规渠道获取受害人信息后进行精准诈骗，作案手法由骗取手机短信动态验证码后实施盗用，向主动诱导受害人发起资金转移转变。为躲避追踪，违法分子丰富了作案的手段和渠道，如通过招收代理和组建工作室的方式，利用会员的收款账户，以高额返佣吸收众多兼职人员，以“跑分”的形式为境外赌博网站以及金融投资诈骗平台提供接收、流转、洗白资金服务。随着科技的加速发展，支付的创新和业务的融合，商家、用户、平台方、电信运营商、第三方支付企业等更多的角色投入到服务中，为欺诈提供更多场景，参与方复杂，业务场景多变，信息呈现不对称、不透明使业务风险具有不确定性和变动性，欺诈风险持续暴露。

2、欺诈技术专业化，攻防难度升级

黑产团伙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黑产使用。欺诈团伙借助大数据等前沿技术，精确识别“欺诈目标”并采取相应措施，攻击更有针对性，黑产社工库欺诈比例上升趋势明显，拖库撞库的操作更为机械化、集中化、智能化，攻防难度升级。红蓝的动态对抗中，黑产也在不断升级进化，欺诈团体的交易行为逐步向僵尸、肉机、团伙的高度伪装形式转移，以规避行方的监控黑产团伙专业化程度不断提升。欺诈方式从早期的简单高频批量操作，进化到在脚本中加入随机时间间隔，避免批量操作过程中呈现出明显规律，从而伪装成正常用户，以绕过平台的简单频度及用户欺诈检测。黑灰产的快速迭代、精细分工、严密协作，使得其可利用新技术和资源进行攻击，且攻击手段在企业安全团队的认知范围之外。

3、诈骗区域境外转移，跨国化日趋明显

移动支付等创新业务迎来发展契机的同时，风险也随之加速从卡介质向移动支付渠道转移。随着政府相继出台鼓励第三方跨境支付业务的政策，第三方跨境支付业务借此时机蓬勃发展。由于跨境支付市场参与主体日渐多元，跨境风险也将进一步蔓延。国内打击不法犯罪力度不断加强，诈骗区域由境内向境外及边境地区转移，作案跨国化特征日趋明显，第三方支付以网络平台为基础，跨境赌博、洗钱等跨境资金非法流动由于资金分散转移，达到规避监管的目的。境外作案不但隐蔽，且数据较难追踪，风险管控与侦测难度日益加大。　在数字支付新业态的背景下，跨境欺诈风险加速凸显。

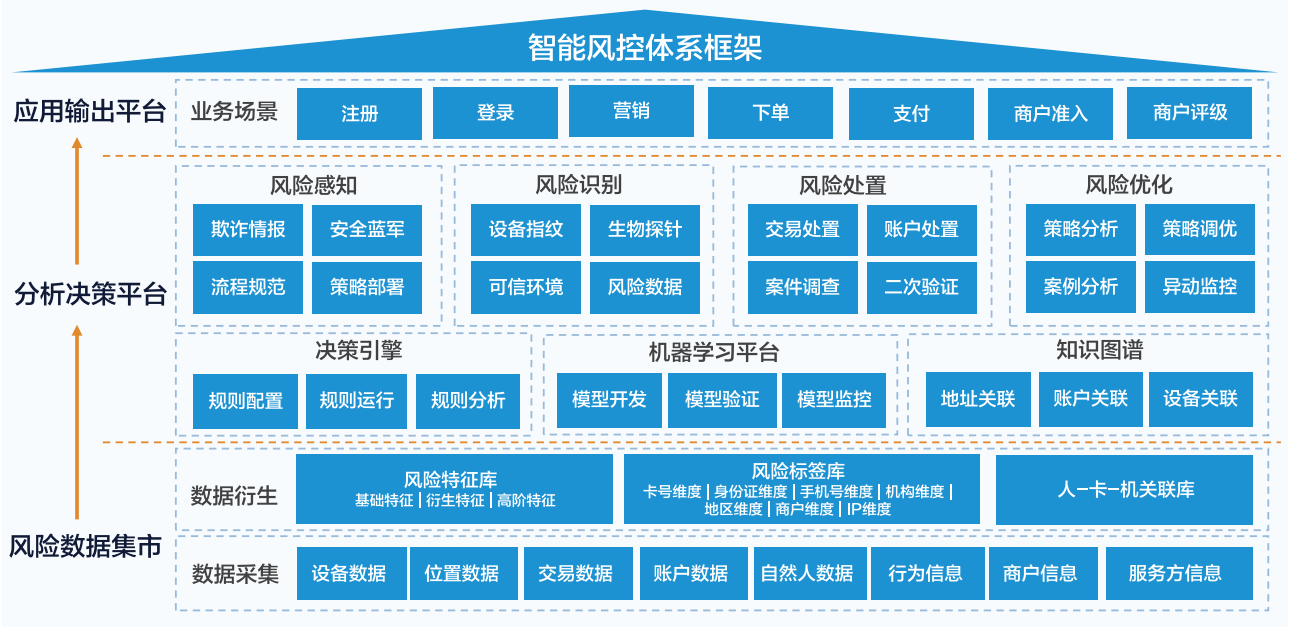


第四章
业务安全生态建设

一、智能风控体系建设

智能风控体系作为风险决策中心，为业务应用提供实时高效的分析决策结果。业务应用既是风控系统的服务对象，又是风控系统业务数据的基础输入源，风控系统需要依据不同业务场景，基于用户行为进行分析，用于后续风险特征、风险标签、人-卡-机关联信息等风险数据的加工。

智能风控体系的建设，需要企业由上至下建立良好企业风险文化，加强风控人员以及业务人员对业务安全的重视。在风控系统建设中，形成事前、事中、事后等诸多环节的监控点，以大数据为依托，应用人工智能等技术手段，通过风控运营实现风险管理闭环。兼顾用户体验的同时，达到风险最低化。小盾安全基于多年黑产对抗经验，归纳总结智能风控体系框架如下，供参考。



1、风险数据集市：通过设备数据、位置数据、交易数据等8大数据维度的输入，全面描述交易主体的行为、关系等属性，进行加工、处理、计算，从而衍生出风险特征库、风险标签库、人-卡-机关联库三大数据衍生库，支撑上层分析决策平台。风险特征是对风险行为的刻画，可直接用于与监测对象比较；风险标签是对某一类特定群体或对象的某项特征抽象分类和概括的结果，标签值具备可分类性。

2、分析决策平台：通过搭建决策引擎、机器学习平台、知识图谱三大基础平台，从风险数据集市获取数据、特征、标签，进行智能分析决策、模型管理及关联分析，对业务交易进行风险感知、风险识别、风险处置和风险优化，以支撑上层业务应用输出。

3、应用输出平台：通过分析决策平台的实时分析决策结果，对用户注册、登录、营销领券、下单支付等行为进行监控并输出监控结果，对商户进行准入审核和交易监控，并根据商户历史交易数据进行商户评级。

三层体系架构，自下而上提供技术支撑，自上而下提供业务指引，三层平台有效联动，构建主动防御、精准识别、联防联控的智能风控能力。

二、行业联防联控

2020年8月，工业和信息化部印发了《关于运用大数据推进防范治理电信网络诈骗长效机制建设工作方案》，将逐步在全国范围内推进反诈大数据平台建设。当前，电信网络诈骗方式和手法不断翻新，诈骗活动呈现从电话诈骗向互联网诈骗、从全国分布向重点边境地区集聚、从“短平快”诈骗向长线套路诈骗转变等趋势特点，技术对抗性日益加大，亟需运用大数据推进构建长效机制，为行业防范治理工作提供更加有力的数据支撑和能力支撑。建立全网疑似涉诈网络资源交叉核验机制，对高危码号、IP地址、域名等及时清理整顿，探索实施行业涉诈失信企业“联防联控黑名单”。运用大数据技术推进构建长效机制，提升平台数据监管能力，为行业防范治理工作提供更有力的数据支撑、能力支撑，将成为打击欺诈不法分子的强有力的手段。

三、消费者权益保护

1、用户安全意识宣贯

在用户端，在安全中心中设计宣传页对用户进行风险教育和风险提示，向用户详细解释网上业务流程、安全控制措施和不法分子的欺诈手法，防止导致用户上当受骗。同时向用户明确提示平台交易的相关的安全风险和注意事项，包括但不限于提示避免设置相同的登录及交易密码，避免将本人登录及交易等敏感信息告知他人，谨防虚假钓鱼链接，注意对敏感信息进行保护等内容。如利用短彩信、微信公众号等方式持续向公众进行防范电信诈骗意识宣贯，及时发布诈骗经典案例和防范措施，加强宣传教育提升用户风险意识。

2、个人隐私数据保护

10月21日，全国人大法工委发布《个人信息保护法（草案）》征求意见稿（以下简称《草案》）。《草案》吸纳了国内个人信息保护的监管实践，并借鉴GDPR等域外法规的先进经验，注重和《民法典》《数据安全法》《电子商务法》等规范的协调。

虽然近年来我国个人信息保护力度不断加大，但在现实生活中，一些企业、机构甚至个人，从商业利益等出发，随意收集、违法获取、过度使用、非法买卖个人信息，利用个人信息侵扰人民群众生活安宁、危害人民群众生命健康和财产安全等问题仍十分突出。客户信息泄漏造成的欺诈案件数不胜数，从电信诈骗、兼职诈骗到交易诈骗，给企业和用户带来资金损失。制定个人信息保护法是进一步加强个人信息保护法制保障的客观要求，是维护网络空间良好生态的现实需要，也是促进数字经济健康发展的重要举措。

数字化时代下，随着消费者的需求更为个性化、场景化，消费者面临的威　胁与挑战更为复杂，对自身权益保护的意识也需要逐步提高。产业机构需要进一步完善消费者权益保护体系，加强联防协作，共同推动解决突出问题，推进线上业务规范创新发展，提升消费者权益保护水平。

第五章
挑战和应对之道

对企业而言，在数字化时代充满机遇和挑战。加强数字风险管理已成为数字经济时代企业提升核心竞争力的重要内容，应当引起企业管理层的高度重视。习近平总书记多次指出，要加快数字经济发展。2020年4月1日在浙江考察时，总书记再次强调，要善于化危为机，抓住产业数字化、数字产业化赋予的机遇，抓紧布局数字经济。2020年5月13日下午，国家发展改革委官网发布“数字化转型伙伴行动”倡议，其中特别提到了要加强数字化生态信用体系建设，维护市场秩序、促进有序竞争。

一、数字风险管理的挑战和变革

在管理模式方面，全方面的数字风险管理不仅仅是合规风险、IT风险，随着服务场景的多元化，企业的业务、管理和商业模式正在发生变化，商家、用户、平台方、电信运营商、第三方支付企业等更多的角色投入到服务中，数字化转型的本质是业务转型，业务风险具体不确定性和变动性，“先找监管规范、再建内控体系，之后合规审计”的传统风险管理模式已不能应对互联网开放的环境，海量的账号和不可控的终端带来的风险，企业应由传统风险管理模式转变为互联网+风险管理模式，以业务安全为中心，进行实时风险分析和决策。

在风控技术方面，在互联网环境下，交易双方的真实身份难以验证，交易信息的真假难以辨别，欺诈行为呈现团伙化和专业化，黑色产业链各环节紧密配合。黑灰产的快速迭代、精细分工、严密协作，使得其可利用新技术和资源进行攻击，且攻击手段在企业安全团队的认知范围之外。为应对和防御黑产，反欺诈技术也必须随之革新和升级。“以技术对抗技术”，是数字风险管理的主要形式。

在风控运营方面，目前企业内部系统互不联通，数据缺乏有效整合，这就使得大量数据被割裂开来，成为一个个数据孤岛，大量有价值的数据资源不能发挥更大作用。数据共享及归一化是实现风险决策的核心，通过数据洞察辅助决策。企业应打破由数据孤岛带来的壁垒，形成集中的数据池，建立数据资产，进而通过数据分析挖掘的手段赋能风险分析和决策，如基础数据质量分析、数据挖掘、风险建模、异常值分析、幸存者偏差、关联分析等，总结风险特征和趋势，实现精细化管理和运营，提升客户体验。

二、数字风险应对之道

为迎接数字化时代各类风险挑战，各参与方应搭建贯穿事前、事中、事后全流程全方位的智能风险防控体系。

1、制定数字风险管理战略，培养数字文化和创新文化氛围。

为应对技术、市场的快速变化，企业需培养数字化思维，建立兼具风险管理和鼓励创新的数字风险管理模式，传统基于简单规则逻辑和经验判断的风险防控手段已不能应对快速变化的风险形势，机器学习、知识图谱技术的的应用为风控行业提供了新的思路和方向。将数据分析结果应用到分析和决策，促进技术变革和创新应用，通过持续的探索学习，培训创新人才，为企业科技赋能。

2、建立风险感知、风险识别、风险处置和风险优化的风控运营闭环。

通过制定风控策略和机制，设计场景化反欺诈规则和模型，建立多重指标体系。线上业务的典型风险场景主要包括用户/账户安全、交易安全、营销活动、电商购物、渠道推广和内容安全等。企业可通过设备ID、IP、用户手机号码，归属地，用户行为、交易时间等多重维度定制反欺诈规则，当业务数据经过风险规则过滤和风险监测模型处理后，根据自身业务要求及风险分析结果，按照不同风险级别采取不同决策，主要包括拦截阻断、人工审核、批准通过。风险决策后，还需进行风险调查、关联排查、案件协查和损失处置的相关后续活动，完善现有风险策略，实现风控流程的闭环反馈优化。

3、提升大数据分析决策能力，完善客户行为和标签体系，以大数据分析为导向进行风险分析和甄别，精细化客户管理。

通过全量数据采集汇聚，全域数据融合，汇集多维度海量数据，对用户进行风险评估，以提供更多元、更灵活的验证方式和手段，引导用户设置个性化风险验证策略，降低用户打扰，提升用户体验。

4、探索创新技术，构建多维决策体系，提升风险决策效率和效能。

企业可利用机器学习模型，对历史数据进行特征分析，如利用逻辑回归、随机森林、SVM、GBDT、XGBoost等不同算法进行模型训练，并将训练后达到要求的模型投入运行，机器学习模型主要应用于异常登录注册、异常交易支付等风险场景。企业还可利用知识图谱从全局关系视角分析和发现问题，知识图谱在事前环节提供了实时关联风险传导、黑产团伙挖掘、风险群体分析、风险群体报告以及风险关联指标输出；在事后环节提供了可视化图关联分析手段，可为风控人员提供案件可视化关联分析及风险追溯、时序分析等风险关联反查服务。知识图谱在现有个体视角风控体系之上，补充了群体关系视角风控手段，主要应用于监控新兴互联网渠道“非面对面、难以追溯”的团伙集团化欺诈。创新技术的应用为构建智能风控体系提供了强大的技术支撑。

扫码关注
了解 AI 如何助力企业智能化转型

www.tongdun.cn ■ 400-068-9796 ■ mkt@tongdun.cn ■