同盾科技
www.tongdun.cn

行业报告

—账户安全保护

同盾科技

目录

1 背景介绍

由于互联网业务的蓬勃发展，互联网风险随之伴生，并“急剧扩张”，互联网企业的每个切面都可能成为被攻击的风险点，如果站在一个服务机构的角度来看，宏观上来说会面临以下几个大类的风险：

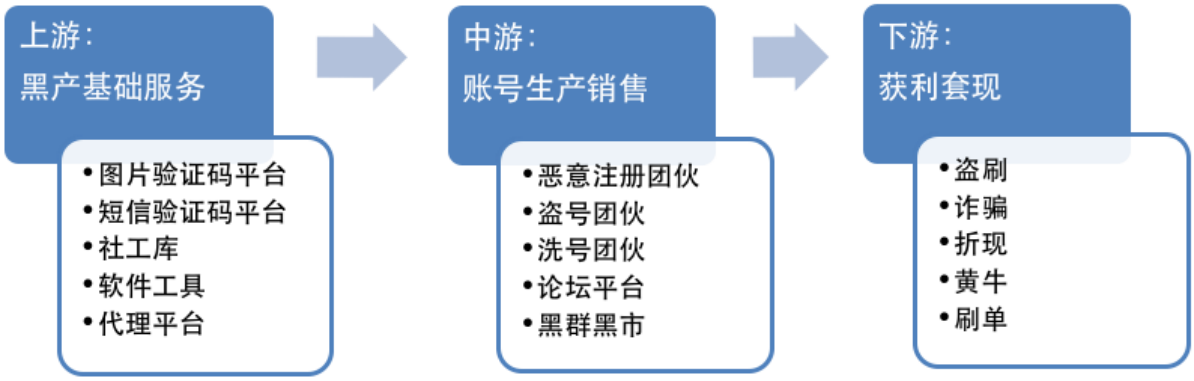
¬ 监管机构关注风险：相关监管机构和部门关注的风险类型，如客户识别类风险、洗钱和恐怖融资风险等；

¬ 基础服务导致风险：一般是指互联网业务风险，因基础构建服务的软硬件系统的原生缺陷，管理不当等原因造成的风险，一般包括IT系统风险、业务流程风险。如系统漏洞、代码泄露等风险；

¬ 经营过程导致风险：通常是指业者在经营服务的过程，因自身经营管理设计的场景、流程、风险偏好等多重原因造成的风险，根据服务与被服务的角色不同分成用户侧风险、商务侧风险、内控风险。用户侧如“骗贷”、“薅羊毛”等不当得利风险，而商户侧如商户“刷单”、广告渠道商的虚假激活等风险，内控风险涉及各种内部违规，伪冒等操作风险；

¬ 外部事件引发风险：一般是指非以上原因因外部事件引发导致的风险事件，非业者过错但是需要业者部分承担损失或配合监控的风险事件，如第三方信息泄露风险、电信欺诈等风险。

这些外部风险极大的影响了企业的正常经营，而且由于互联网业务天然的非面对面交易，以及通过技术手段伪装等特性，给平台方的风险防控制造了很大的困难。



整个互联网欺诈已经形成了完整的产业链条，即上游提供“专用工具”和“专用物料”，帮助实施欺诈的人员对各种风控技术和手段，提供专业的服务和技术支持。而中游则会针对特定的行业或者特定

的机构，利用外部工具以及对客户经营策略、风控的偏好等进行深度研究，进行定点的“行业深耕”。而欺诈人员为了规避“经营风险”，则会整合下游人员用技术手段、工程众包等社会化分工的方式“拉拢”更多人员进行攻击。

总体来说，风险发生具有主观性、欺诈种类多、发生频率高、欺诈手段更新快的特征。

•主观性

欺诈风险和一般的市场风险不同，它是由人的主观行为构成的风险，其动机多种多样，除了一般直接和间接经济利益的驱动以外，还有如技术炫耀，情绪发泄等多样的不理性行为，因此解决起来面临的问题更加复杂。

•欺诈种类多

在互联网服务领域，欺诈可谓是无处不在。无论是对传统的金融机构还是新兴的互联网应用，都存在相应的金融欺诈方式。

•发生频率高

随着移动4G网络的普及，O2O服务、手机购物和移动支付等业务的快速发展，用户在线支付等活动越发频繁，同时越来越多的用户信息通过互联网上传给各类应用服务商，进而加剧了网民隐私信息泄露的风险，这两点综合起来提高了发生金融欺诈的频率。

•欺诈手段多样且更新快

金融欺诈不但种类多种多样，而且其更新速度也很快。通过技术手法进行破解、服务攻击、第三方攻击，利用社工方式、社会热点事件、人性弱点等进行欺诈和隐私信息的获取，或者多种攻击手法的组合使用。

对于提供互联网服务的风控服务商来说，要担心的问题并不是攻击是否会发生，而是何时会发生。构建无懈可击的防护是不现实的，但是可以通过限制攻击者的行动空间、提升攻击者的攻击成本，来抑制其对资产的危害，从而最大限度降低风险和威胁的影响。

2 风险报告简介

同盾科技成立于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与分析决策服务提供商，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。同盾通过持续创新产品与技术，不断提升服务可靠性，将人工智能技术深度应用到金融和互联网风险管理和反欺诈领域，经过几年的发展，同盾已经是全行业增速最快的企业，目前已有超过10000家企业客户选择了同盾的产品及服务。

本报告研究时间选取区间为2017年6月-2018年6月，研究对象包括银行、保险、互联网金融、消费金融公司、电商、游戏、O2O、航旅、社交等若干行业，通过百亿交易数据取样，对行业中注册风

险、登录风险进行宏观性的描述。因为从业务流程上看，账号安全保护是互联网风控的第一环，也是最基础、最重要的一环。由于篇幅的限制，后续同盾科技反欺诈研究院会持续对于营销、绑卡等风险事件或者电商、O2O等行业进行专题分析。

3 账户安全综述

3.1 账户安全存在的常见风险

a) **垃圾注册**

平台新业务上线之初，常常进行拉新优惠活动，而“羊毛党”通过虚假手机号等方式绕过平台验证，批量套取优惠，给平台造成不必要的资金损失，降低营销效果。

b) **拖库撞库**

网络欺诈分子利用互联网中大量泄漏的用户名密码进行尝试，如果平台账户密码不幸在泄露库中，那么可能会导致用户信息及资金蒙受损失。

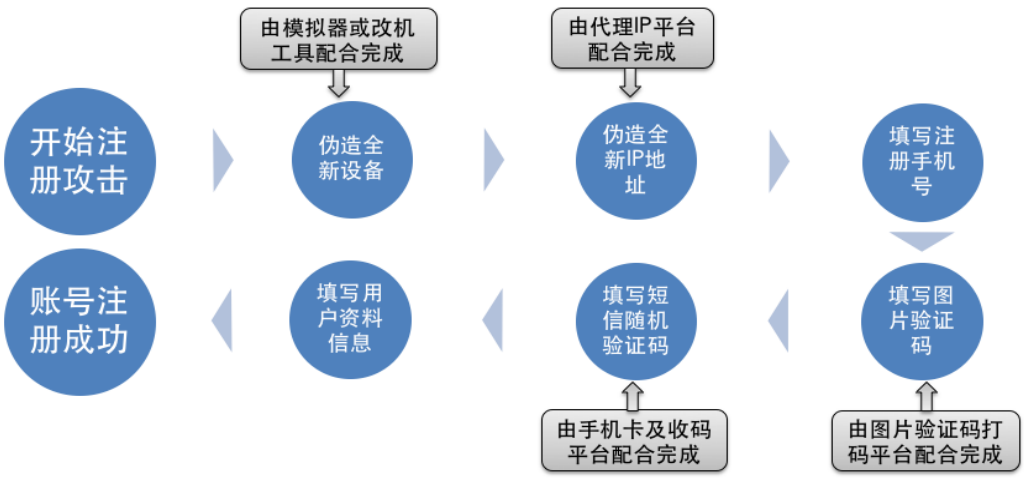
c) **鱼叉攻击**

用户因为中网络木马钓鱼导致账户密码泄露，进而导致账户的资金损失及企业形象受损。

d) **暴力破解**

网络欺诈分子会通过机器对账户密码进行暴力破解，进一步获得账户登录权限，导致用户资金损失和企业品牌受损。

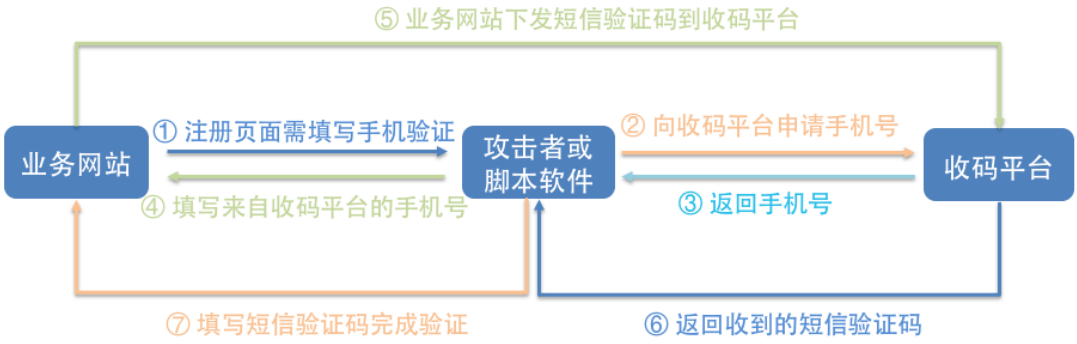
3.1.1 垃圾注册机器欺诈流程



3.1.2 识别图片验证码流程

- 真人识别图片验证码收费0.01元/次至0.25元/次，人工智能识别平台准确率在98%以上。

3.1.3 破解短信验证码流程



手机短信验证码收费0.1元/次至3元/次，相对于使用实体手机卡成本更低。

3.1.4 拖库撞库

近年来，随着频繁出现的数据库泄露事件，撞库攻击取代了木马盗号成为了主流的盗号方式。据统计，能够成功绕过风控的攻击占供攻击量的83%，撞库的成功率则在0.4%左右浮动。

- 2014年某火车票售卖平台网站由于撞库攻击导致131653 条信息被泄露，包括用户账号、明文密码、身份证和邮箱等；

- 2016年某云计算服务平台遭撞库攻击50万账号被盗，胡某通过撞库软件批量登录百度账户，筛出正确账号密码50余万条；
- 2017年俄罗斯黑客利用恶意软件RouteX，感染美国网件路由器实施撞库攻击；2018年英国彩票公司Camelot疑遭撞库攻击，1050万彩民被通知紧急修改密码；
- 据国外某安全组织公布的数据，截止 2018 年 9 月 30 日，全球互联网累计泄露的用户数据累计超过 55 亿条。

（素材来源威胁猎人：2017年度互联网黑产报告）

撞库流程

撞库的数据来源：黑客盗取的数据库、地下黑市交易等；

撞库的攻击分布：地域上，有57%的攻击来自于中国；行业上，有63%的攻击是针对游戏行业；

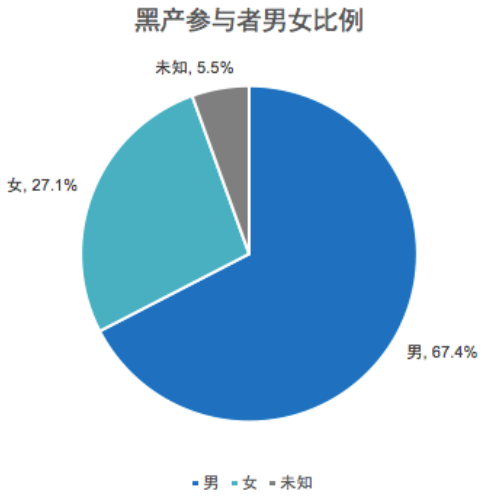
撞库的技术手段：脚本访问、软件工具等。

4 风险现状

4.1 黑产群体分析

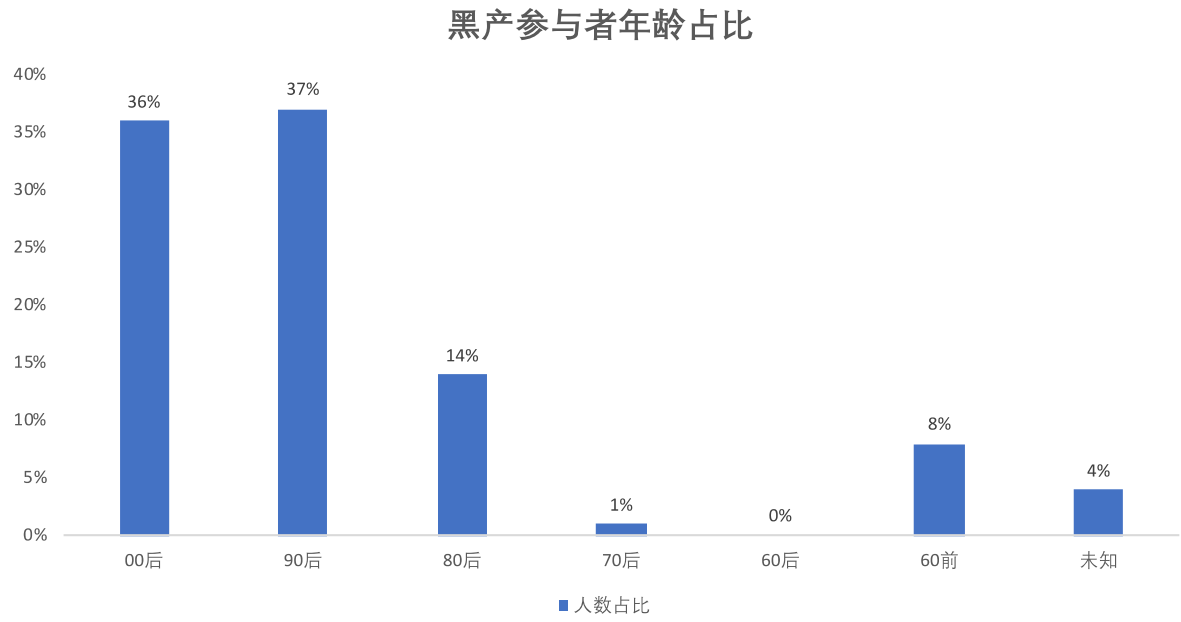
考虑到大多数的黑产是通过QQ群聚集在一起，因此通过对QQ群组群成员的样本分析，报告对黑产群体分布进行了统计。

4.1.1 性别比例



根据CNNIC数据，截至2017年底中国网民男女比为52.6：47.4，但是通过统计分析发现，在黑产领域67.4%的人群是男性，占据了总统计样本的2/3，说明在整个黑产行业中，男性风险远高于女性。

4.1.2 年龄层次



截止2017年底，00后（8-18岁）网民占比约为19.6%，90后（18-28岁）的网民占比30%，80后（28-38岁）的网民占比为19.6%，而在参与黑产的年龄统计分布上看，00后（8-18岁）与90后（18-28岁）占比最多，分别有36%和38%，80后（28-38岁）位居其次，有14%，其余年龄段均不足10%。

通过以上数据看出参与黑产的人员当中，28岁以下的年轻人是黑产的主力军，占据了总体约74%，且黑产人群参与度出现逐步向年轻人倾斜的趋势，00后（8-18岁）年龄段网民中黑产参与度远远高于其他年龄层，而其表现会随着年龄的增长逐步递减。

在60前（58岁以上人群）中占比约8%，虽然个别数据出现一定的集中度，但是人群分布中没有特别集中化的表现，推定这部分人群可能是因为数据泄露，“被参与”了相关事件。

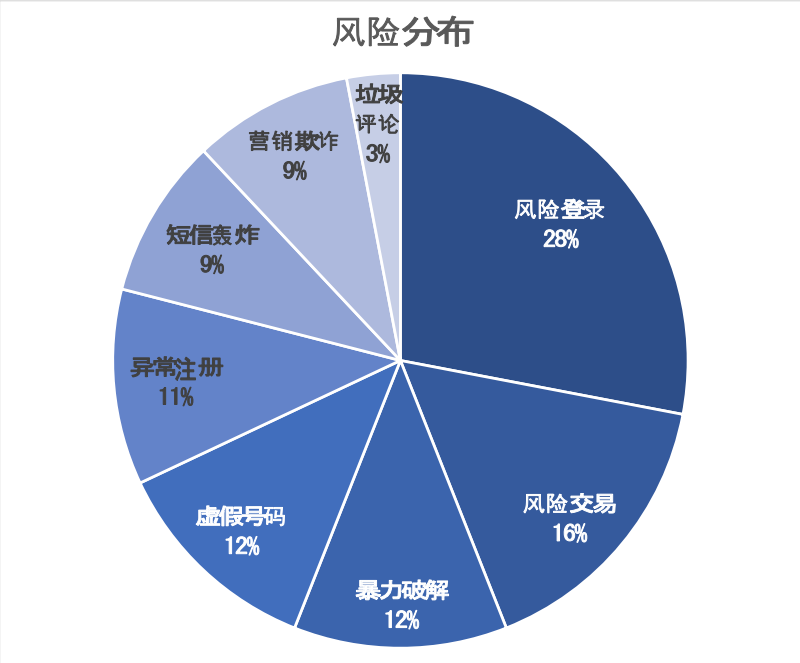
4.1.3 地域分布

通过对样本的统计，黑产成员分布的地区主要是广东、北京、山东、河南等，占比分别为6.36%、5.51%、5.32%、4.81%。而黑产群的归属地在广东省最多，达到26.5%，其次是上海市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%等。

（素材来源：同盾与FreeBuf联合发布的《深渊背后的真相之“薅羊毛产业”》报告）

4.2 宏观风险分布

本报告选取2017年6月-2018年6月的一年内，通过对银行、保险、互联网金融、消费金融公司、电商、游戏、O2O、航旅、社交等行业。百亿交易数据数据取样，对行业中注册风险，登录风险进行宏观性的描述。



通过上图宏观数据取样可以发现，登录风险，即账户安全类风险依旧是当前面临的最大风险，总占比在所有的风险表现中高达40%。因为利用泄露的数据，或者直接对账户进行破解，或者通过技术手段进行伪装登录是获取潜在利益最短的攻击路线，所以站在黑产的角度来说有直接获利的可能，即使无法直接获取利益，通过对数据的“采集”还可以在其他平台进行二次攻击，或者直接将数据进行转卖。所以这是收益最大、攻击行为隐蔽快速、攻击成本相对较低的一种获利方式。

登录风险包括风险登录和暴力破解两种风险类型，风险登录是指在登录过程中其行为有异常性表现，如操作行为异常、时间异常、地理位置异常等风险情况，而暴力破解包含正向和反向两种方式，即同一个账号更换不同的密码信息，或同一个密码信息更换不同的账号信息。

在经营过程中产生的风险，总占比在所有的风险表现中达到37%，报告主要统计了以下四个维度，包括短信轰炸、营销欺诈、风险交易和垃圾评论。特别是短信轰炸、营销欺诈以及垃圾评论的比重有所上升。

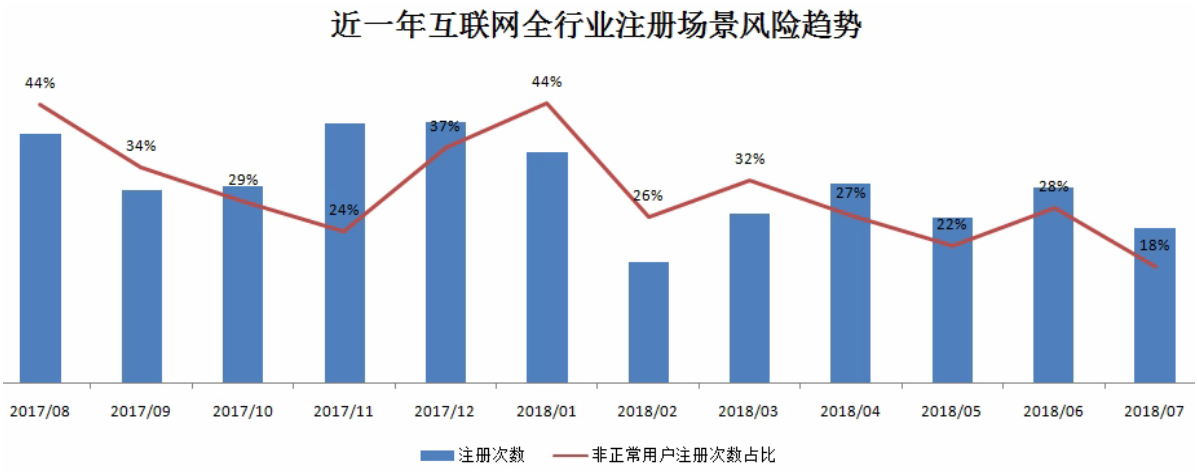
短信轰炸是指攻击者利用外部的短信接口，以机器的方式频繁调用业者的短信通道从而降低服务响应，徒增成本的一种攻击形势。而营销欺诈多发生在进行外部的营销推广过程中，利用虚假下载、虚假安装等方式能够更多的获取虚假营销成果、更多结算费用，这种欺诈行为一般是渠道商参与其中，并且对服务方的营销风控有一定程度的了解。在同盾科技服务的客户案例中，还发现个别内部人员参与其

中，共同获利的情况，危害极大；而垃圾评论这种风险虽然占比只有3%，但是涉及内容为客户发送的内容，涉及敏感信息，这类风险虽然相对偶发，但因其内容会影响到正常客户的良好体验，甚至有可能会引发监管部门的关注，极大的危害了平台的声誉，进而可能引发持续运营的风险，所以也需要高度关注。

注册类风险占据所有风险事件的23%风险份额。伴随着国内互联网业务的快速发展，平台之间的竞争非常频繁，类似“发放红包”、“饥饿营销”、“组团购买”等各种市场促销活动层出不穷，平台为了扩大新客户的增长、保持老客户的活跃，在活动方面投入了巨额的资金。在攻击方看来，只要能够掌控足够多的账户信息，增加频率，即可获取可观的收益，从注册新用户获取红包，到后续参与抢购、抽奖，商家评价等各个场景之中均可获取巨额利益，加之部分平台在一定程度上对此类风险容忍度较高，并且此类风险事件攻击者的社会处罚成本极低，也纵容了此类风险事件的频繁发生。在注册类风险中，主要包括“虚假号码”和“异常登录”两种风险形式，特别是虚假号码这种通过外部平台购买大量的手机号码，从而进行获利的风险形式，在注册场景下其权重已经超过51%，而且有更加恶化的趋势。

4.3 全行业近一年风险情况

4.3.1 注册场景维度



中国互联网协会《2018中国互联网发展报告》中指出，截止2017年底，中国网民规模达7.72亿，相对2016年新增网民4074万人，总体增幅约为5.27%，但是因为是随机选取数据的原因，所以从上图可以发现，在注册场景下，17年9月虽然出现一定程度数量的下滑，但是从9月到12月出现逐步增加的态势，而18年的单月注册次数比17年的注册次数总体有所下降，

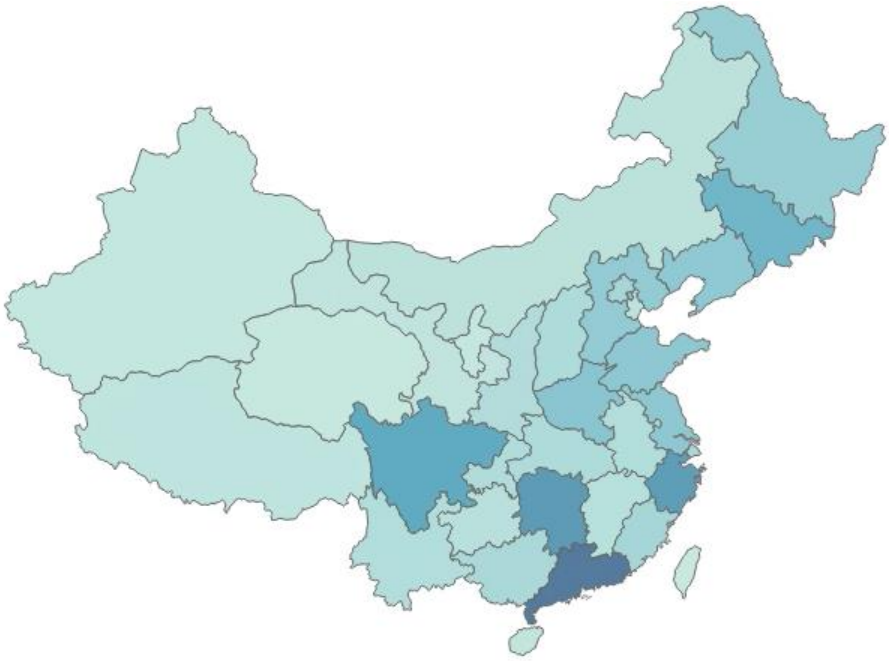
从总体的情况来看，一年非正常用户的登录次数占比约为30%，也就是说，平均每10次注册，就有3次属于高风险注册，并且注册类的风险事件与注册事件的总量存在一定的正相关关系。

非正常用户注册次数占比在17年8月和9月、17年12月和18年1月出现两次大的上升，特别是在17年8月和18年1月，来到了最高点，接近一半的用户出现非正常的注册风险事件，这两个时间点中00后（8-18岁）年龄段网民中黑产参与度远远高于其他年龄层，这样的一个产业人群覆盖存在一定的时间关联性。

基于IP地址的风险分布

注册场景下的高危IP主要来源是广东省，其次是浙江省、江苏省。这与之前对于地域分布情况的判断也基本吻合。

基于手机号码的风险分布



注册场景下的高危手机号主要来源是广东省，其次是浙江省、湖南省、四川省。同样也与之前地域分布的结论相吻合。

4.3.2 登录场景维度

下图是从2017年8月至2018年7月，抽样选取的全行业登录场景下的风险表现趋势：

上图可以发现，全行业的登录场景登录次数基本保持稳定，但18年的月风险表现要明显高于17年的风险，非正常用户登录次数占比平均在20%左右，换句话说就是每10次登录就有2次是高风险登录，与注册场景不同的是，登录场景的风险在5月份达到峰值。

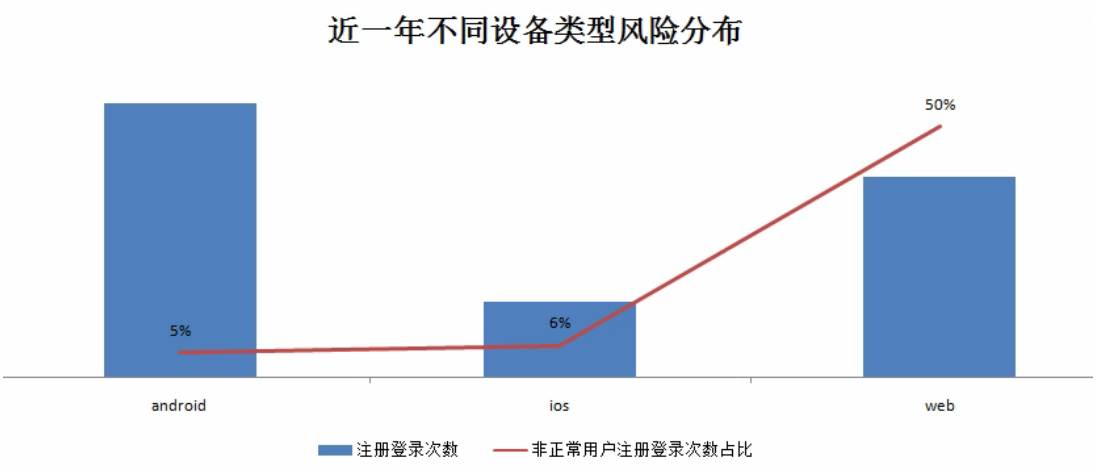
基于IP地址的风险分布

与注册场景不同，登录场景的高风险IP主要来自于江苏省，其次是浙江省、四川省等。

基于手机号码的风险分布

登录场景下的高危手机号主要来源同样也是广东省。

4.3.3 智能设备维度



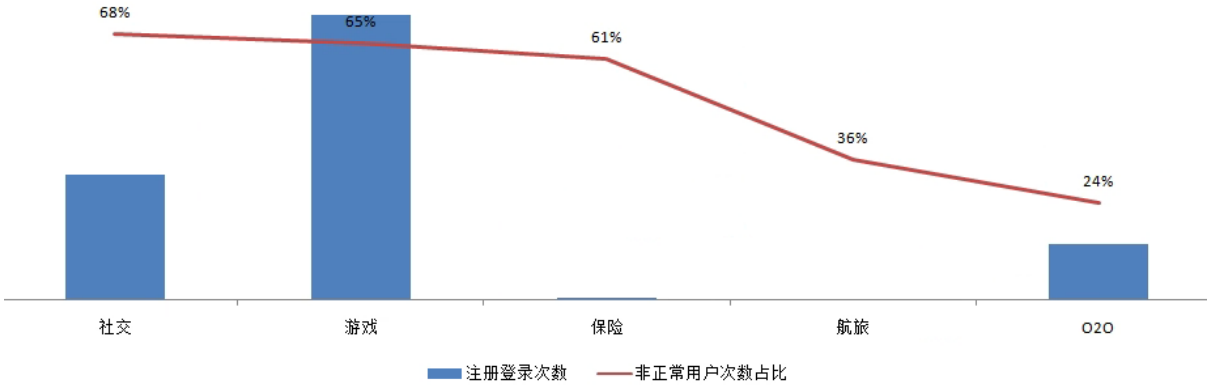
从设备类型上来看，安卓与IOS的风险比较接近，但注册登录次数上安卓要远高于IOS，风险最高的是网页端，非正常用户注册登录次数占比高达50%。

从这部分数据来说，目前在设备端行业通常以设备指纹技术为主要的防控技术手段，但是客观来说，因为Web端部署的H5设备指纹在防破解能力、代码混淆、算法加密等方面相对于APP端较弱，所以Web端在风险防御方面具有一定的天然短板。需要特别提醒的是，同盾发现很多机构在Web端的H5设备指纹，使用的技术是基于开源的设备指纹技术，即使做了一定的客户化处理，但是由于其工作原理、取数逻辑、加密算法等都是公开的，所以其防御能力还是非常有限的。

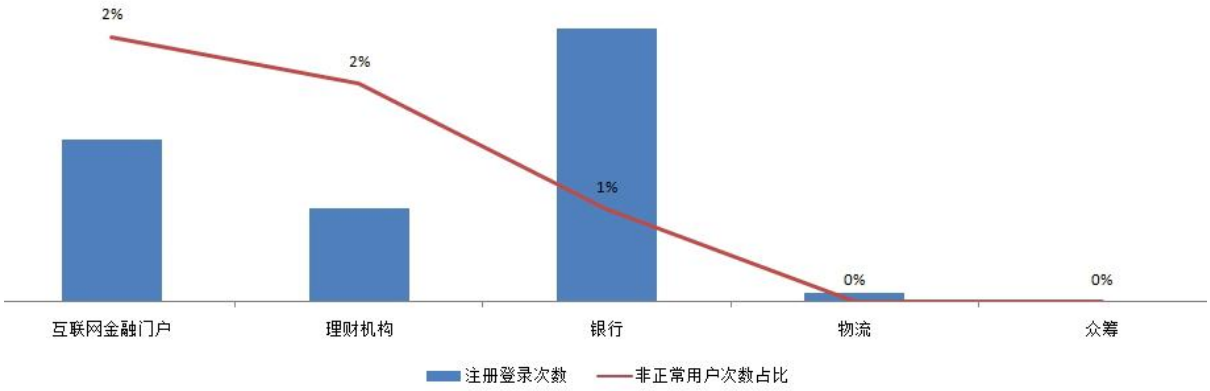
4.3.4 风险行业统计

整个互联网行业中风险是广泛分布的，根据服务机构背景、IT技术攻防能力、风险获利的性价比综合评估，从风险管控能力以及黑产工具的成熟度来看，不同的行业指间还是存在相当不同的风险表现。根据抽样的业务数据显示，行业表现具有较大的差异（以下数据仅统计了行业当中风险发生的次数，并非实际造成的风险损失金额）

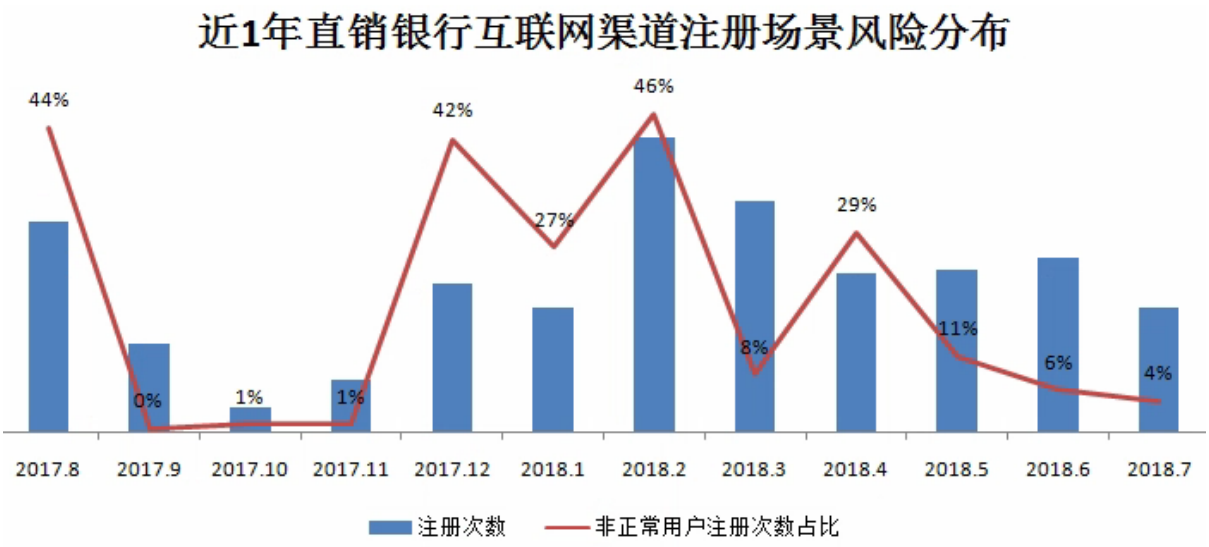
发生风险次数占比最高的前五个行业分别是：社交（68%）、游戏（65%）、保险（61%）、航旅（36%）、O2O（24%）。



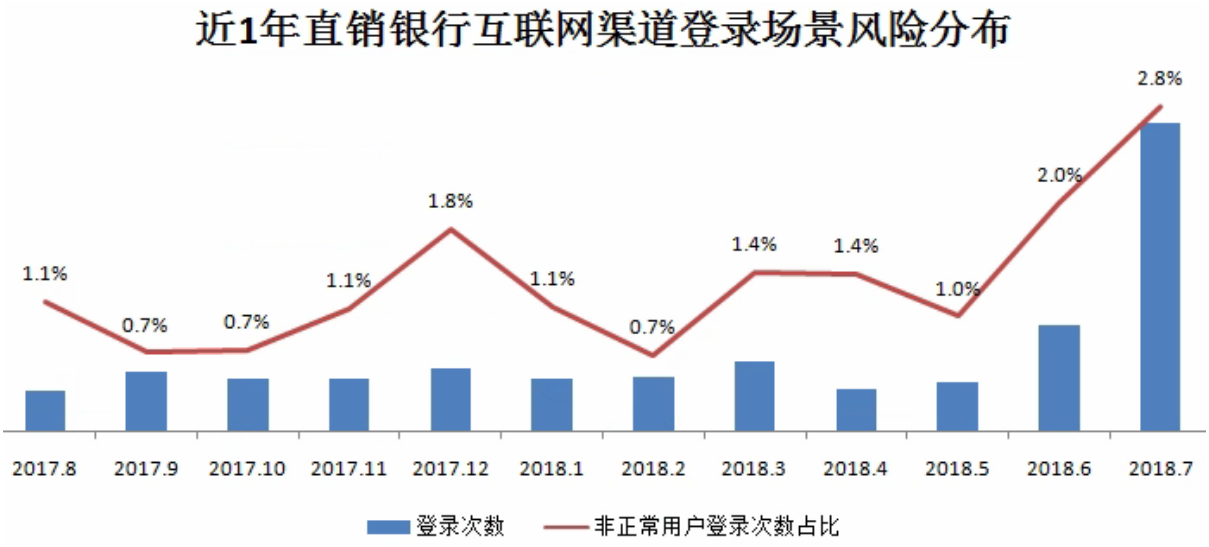
近一年以来，互联网账户按行业汇总，风险最低的前五个行业分别是：互联网金融门户（2%）、理财机构（2%）、银行（1%）、物流（0%）、众筹（0%）。



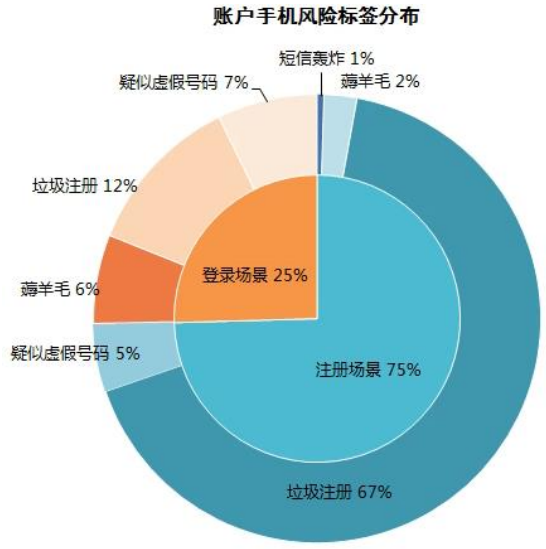
4.4 银行行业互联网渠道近一年风险情况

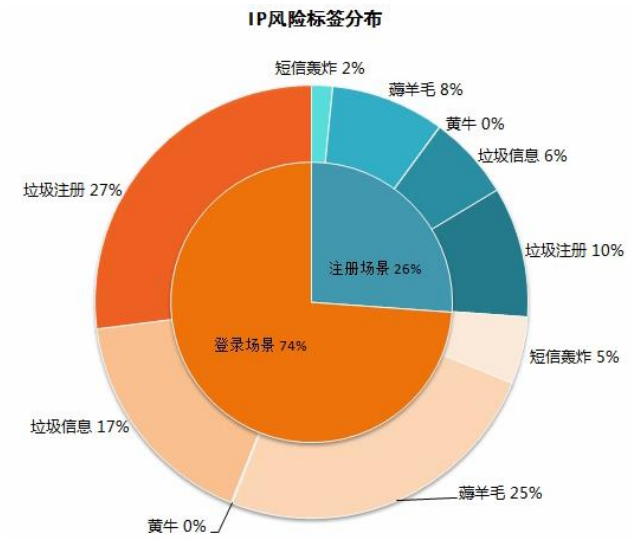


- 寒暑期直销银行往往会推出营销活动吸引新用户注册，导致账户注册量在2017.8及2018.2期间有明显上涨；
- 营销推广期间，黑产作弊形势严峻，风控非正常用户注册占比上升至46%；
- 由于直销银行账户注册身份校验相对严格，故行业注册场景非正常用户注册占比相对于全行业略低。

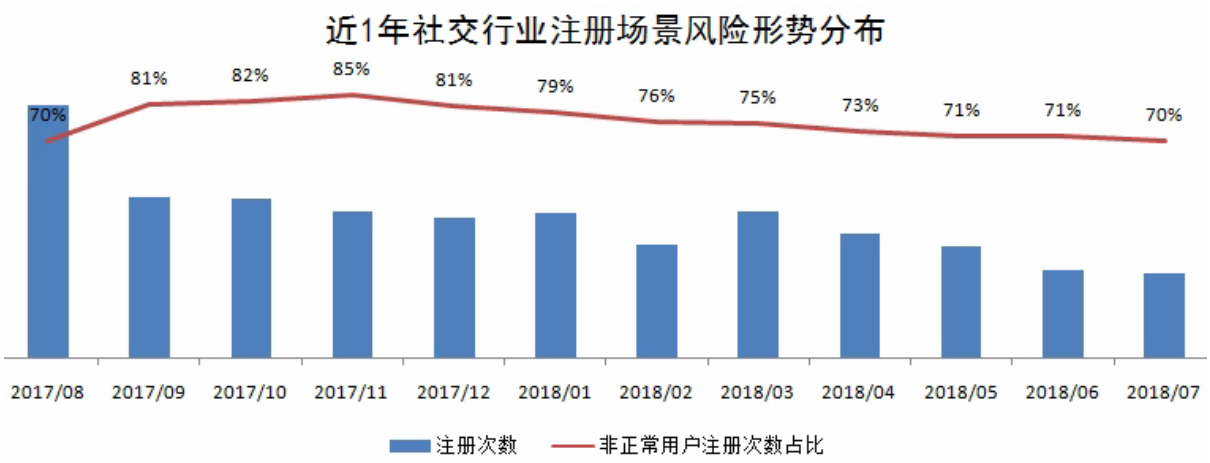


- 在登录场景的风险识别率较注册场景要偏低，主要是由于在登录场景，黑产对银行的攻击风险以及违法成本相对于社交、游戏等行业要高很多。

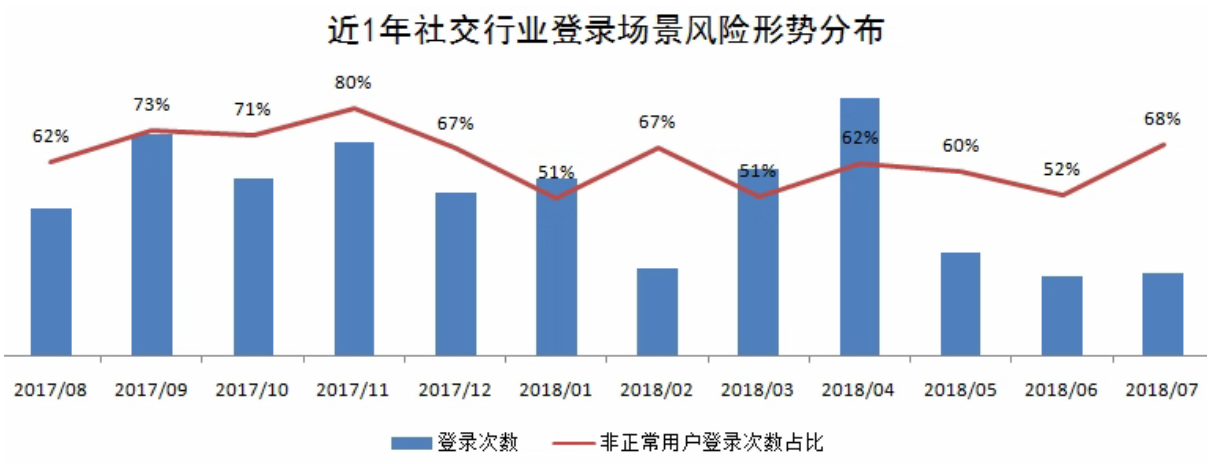




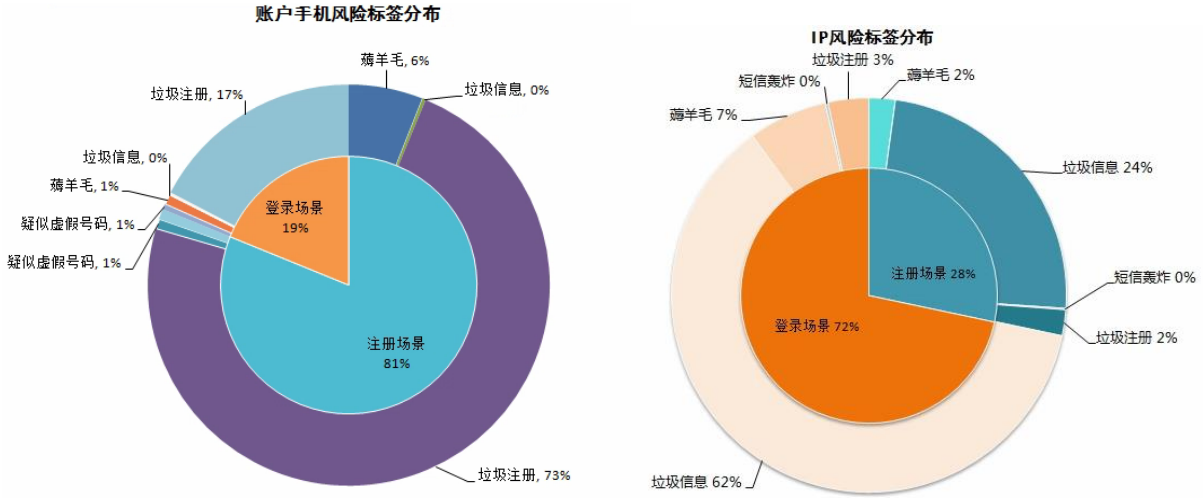
4.5 社交行业近一年风险情况



在风险最高的社交行业，可以看到近一年的注册场景非正常用户注册次数占比都比较平稳且维持在70%以上，18年的注册次数以及风险相对17年略有降低。



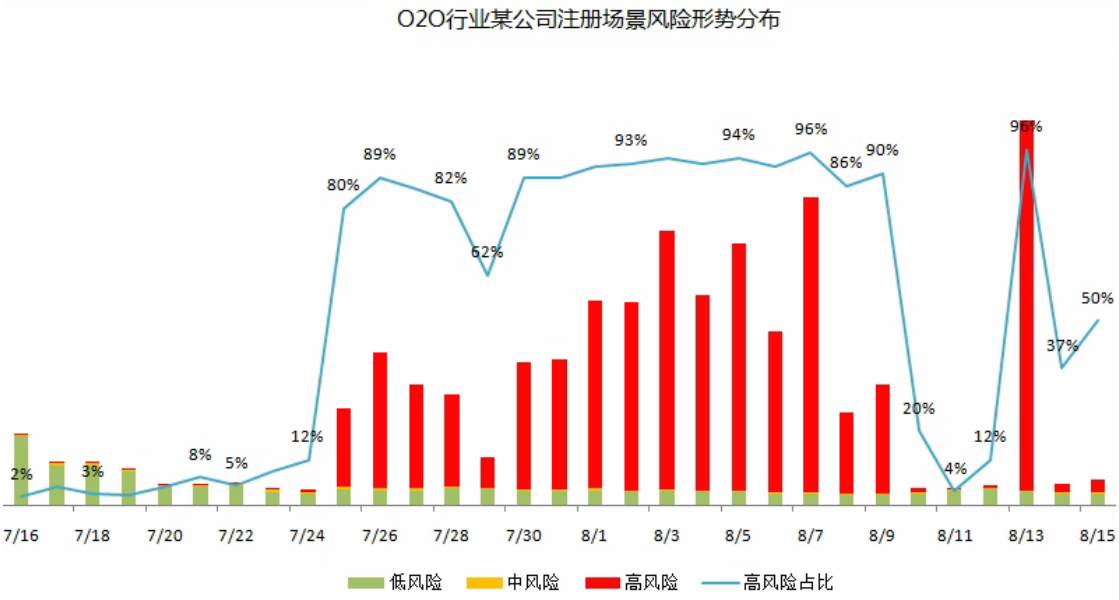
而在近一年的登录场景，非正常用户登录次数占比有所波动，但仍都在50%以上，平均在65%左右，登录次数方面18年相比17年也有所降低。



5 案例分享

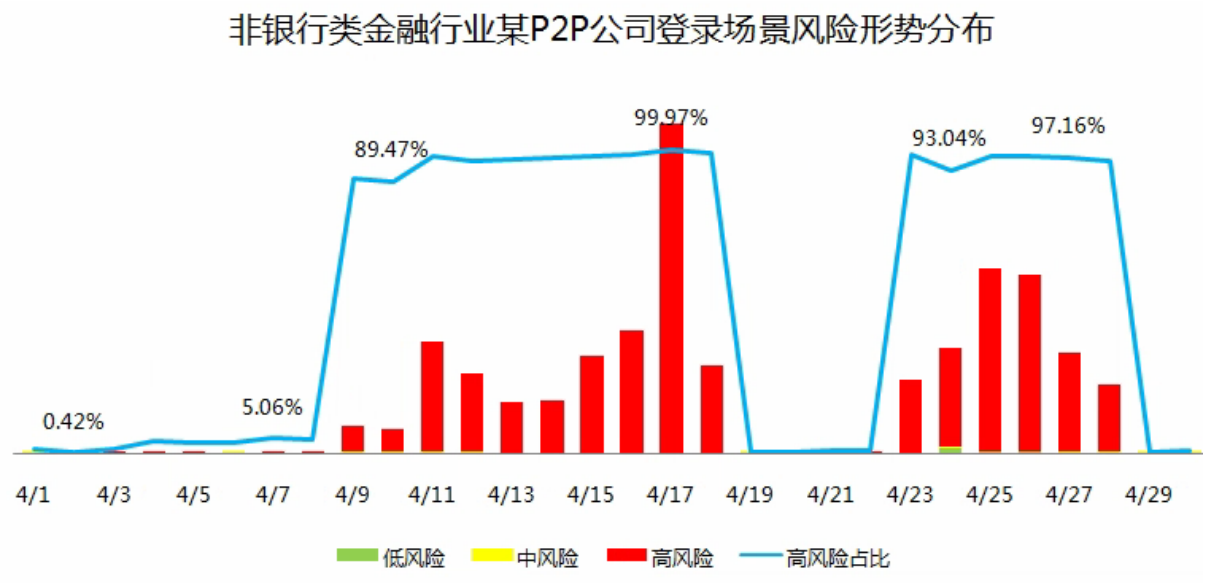
5.1 垃圾注册案例

2018年7月至8月O2O行业某家公司发现某应用端突增大批量的新注册用户，且这批用户经同盾的风控决策引擎、设备指纹信息、虚假号码黑名单等强有力的工具判断发现，有平均90%以上的新注册账号为严重异常注册账号，可以判断该公司遭受到了大规模的黑产批量垃圾注册攻击。考虑到该公司对新人的奖励优惠力度极大，此次拦截替公司挽回了上千万元的直接或间接损失。



5.2拖库撞库案例

2018 年 4 月非银行类金融行业某公司的登录总次数及高风险识别率大幅上升，该公司 4 月总登录次数千万余次，其中 98%以上是撞库攻击，同盾拦截率在 99%以上；约 17 万手机号被同盾检测为虚假号码，并且另有大量手机号曾在其他多家 P2P 公司进行过注册登录，疑似数据泄露导致本次攻击。



在本次攻击期间使用的设备中，同盾设备指纹检测到，约85%的调用所使用的设备存在参数异常的情况。从IP情况看到本次攻击IP关联多账户发起调用，且IP归属地主要集中在山东、江苏、河南，与之前同盾发布的《薅羊毛产业报告》中分析的薅羊毛群数据情况吻合。（QQ羊毛群地域分布详情请参考同盾科技公众号2017年11月发布的《黑镜调查：深渊背后的真相之“薅羊毛产业”报告》）

写在最后

本报告由同盾科技反欺诈研究院编撰而成，报告中所涉及到的数据来自网上公开数据，使用合法合规技术手段、深度调查以及抽样调查等方式获取。报告中所提及的案例均取材于同盾科技为客户提供的反欺诈服务过程中，所实际呈现出的信息。

同盾科技反欺诈研究院是同盾科技最新成立的“智库”级研究院，对于反欺诈领域的学术探讨、理论研究具有非常积极的意义，同时对于产业实践也有现实的指引作用。反欺诈研究院的成员均来自于反欺诈领域内的顶级专家精英，不仅拥有丰富的行业经验，同时通过在行业内长期的浸润，对于行业的整体脉络的把握，存在的痛点，以及未来发展的趋势均有独到的见解。

同盾科技反欺诈研究院将会持续聚焦，致力于围绕反欺诈进行全方位、多角度的调察和研究，以系列报告的形式定期发布，基于反欺诈研究院对行业深入研究，利用调研数据和权威部门相关资料，再结合同盾科技在前沿应用中所沉淀下的经验。 系列报告将尽可能系统和科学地反映出反欺诈领域的技术热点、场景应用、产业发展现状以及行业未来趋势，为推动反欺诈技术创新和行业健康发展提供重要的决策参考，为构建网络诚信生态提供“同盾智慧”和“同盾方案”。