2015数据风控年报

阿里聚安全

阿里安全开放平台

摘 要

- ✧ 网络欺诈催生黑色产业链，商业运作模式日渐成熟。互联网+的飞速发展催生了“黄牛”、“打码手”、“羊毛党”等日趋专业的黑产团伙，他们分布在产业链的各个环节，为黑产利益链条提供基础服务。
- ✧ 2015 年黑产收入数千亿，从业人员多集中在沿海省市，他们具备专业攻防能力、100%精力投入、完整的产业链结构和分工、各种先进的工具。企业和开发者与黑产之间是一场实力悬殊的战争。
- ✧ 作为上游，图片及手机验证码平台为黑产提供原材料，用以突破注册环节的验证，为产业链下一步提供账号支持。2015 年手机验证码平台充值人数同比上涨 300%、充值金额同比上涨 260%，涨幅迅猛。
- ✧ 作为中游，黑产通过恶意注册和盗号为利益套现做准备。黑产通过图片验证码、手机验证码等平台批量注册账号，或在登录环节撞库、拖库进而非法获取账号，并通过垃圾账号分销平台销售给产业链下游，为利益套现做准备。
- ✧ 作为下游，黑产通过活动刷单、欺诈、盗窃、勒索进行利益套现。以活动刷单为例，当今互联网环境下，刷单现象严重是，刷单利润率高，行业分工越来越细，逐渐成为支柱性的黑客产业链，其中热门活动被刷的概率 100%，这些被刷的资金直接流入黑产，未对企业或正常用户产生任何价值。
- ✧ 未来数据风控形势依旧严峻。“人肉”、“社工”模式规模将扩大，风险识别需要更多的结合用户行为做综合判断。“实时化”风险识别能力需要增强，以快速响应与黑产的攻防战。“多样化验证”将成为主流，更好地平衡安全与体验。

目 录

第一章 2015年数据风控回顾

2015年电商、网游及互联网金融飞速发展，各种创业公司通过活动形式的补贴来获取用户、培养用户的消费习惯，但高额的补贴、优惠同时也催生了“黑色产业链”，由“黄牛”、“打码手”、“羊毛党”组成的团伙已经形成了专业化组织，从业人数过百万，他们内部有着明确分工，严重破坏了商业活动的目的，侵占了数以亿计的活动资金，使正常的用户享受不到活动的直接好处，这些行为距离欺诈只有一步之遥。

2015年的网络犯罪也变得更加专业化、规模化、组织化，国内外各行业出现信息泄露引起的重大安全事故20余起，有账户风险的用户量超过十亿。

互联网在改变传统商业的同时，同样也使以欺诈、偷窃等方式来获取利益的恶意行为甚至犯罪发生了根本性变化；利用互联网分布式信息可以同步共享的能力，让“黑产”参与方之间可以实时、多方、多角度地互动沟通。这种网状、协同方式是相对于传统犯罪链最大的优势，除了专业的“黑客”、“黄牛”，这个网络还连接了万倍的外围成员，他们所做的事仅仅是“打码”、“发短信”、虚假交易、不符合实际的评论，轻松获利。

第二章　互联网业务黑色产业链分析

目前黑产的日交易额可达数亿，但这仅是冰山一角，那些冰山下的更为复杂隐蔽，黑产的整体规模难以估测，其未知的能力更让人恐惧。

2.1　黑色产业链综述

黑产现如今已经有了十分成熟的商业运作模式，产业链复杂、隐蔽、高效，是一个紧密结合的复杂链条。

在产业链的上游是一个基础性的环节，承担着挖掘、制作生产和供应的职责，支持着众多类型的网络黑产，为其提供重要资料。黑产的上游包括提供验证码识别服务、手机验证码服务平台、自动化的软件工具，以及为黑产提供身份信息与账号生产原材料的社工库等。

中游是网络账号提供商及交易交流平台，在产业链中充当账号生产者和各种服务提供者的角色，是沟通上下游的桥梁。

产业链的下游主要是利用非正常渠道的网络账号进行欺诈、盗窃、刷单等恶意行为的团伙，他们冲在最前线，与网络用户正面交锋，给用户带来直接的利益损失。

图 1　网络黑色产业链全景图

黑产人员以 17 至 21 岁的男性为主，主要分布在江苏、广东、浙江、山东等沿海省份，这也符合经济发展水平和人口密集度的分布。

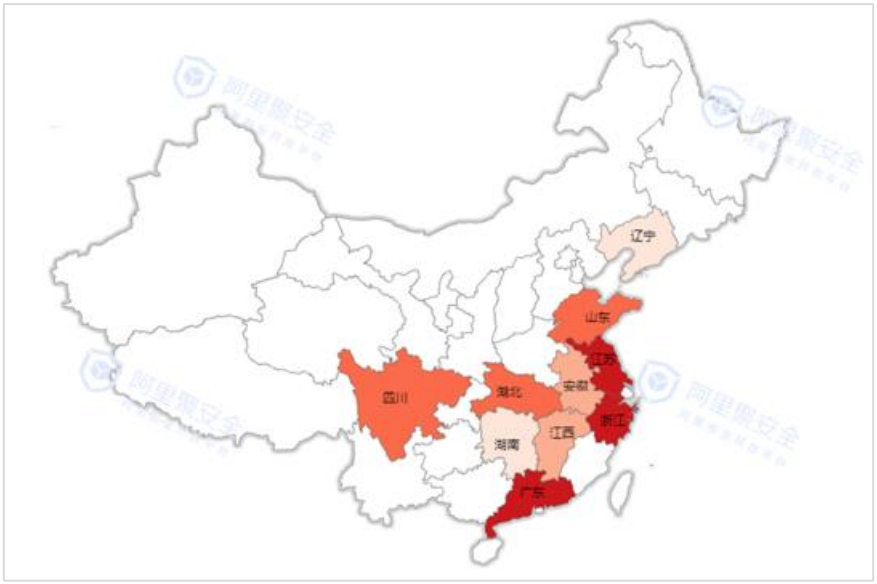

图 2 黑产从业人员的 Top 区域分布

相比 2014 年，黑产在今年总收入千亿级，手机验证码平台相关黑产总收入最高，刷单平台相关黑产人均收入最高。

黑产具备专业的攻防能力、100%精力投入、完整的产业链结构和分工，及各种先进的检测工具等，而企业或开发者没有相应的安全攻防经验、没有精力和时间投入到安全攻防中，导致他们之间是一场没有硝烟、实力悬殊的战争。

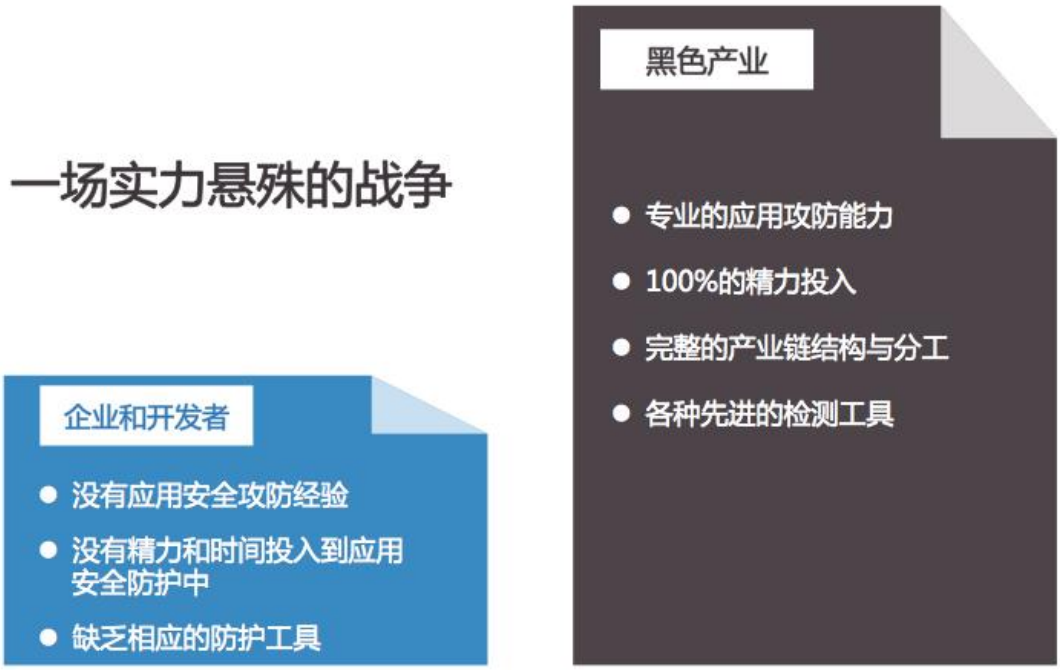

图 3 企业和开发者与黑产之间是一场实力悬殊的战争

2.2 黑产上游：打码平台、手机验证码平台、黑产软件

1. 打码平台（图片验证码平台）

很多网站都会通过图片验证码来识别机器行为，对非正常请求进行拦截。因此打码平台已成为大多数黑产软件必备的模块之一，为黑产软件提供接口，突破网站为辨别机器还是人类行为而设置的图片验证码。

黑产组织社会低收入人员在打码平台上人肉识别图片验证码(每个仅需 0.001 元至 0.25 元)，便可轻松绕过图片验证码的防控。2015 年，打码平台的充值客户数比 2014 年增长了 27%，充值金额增长了 40%。

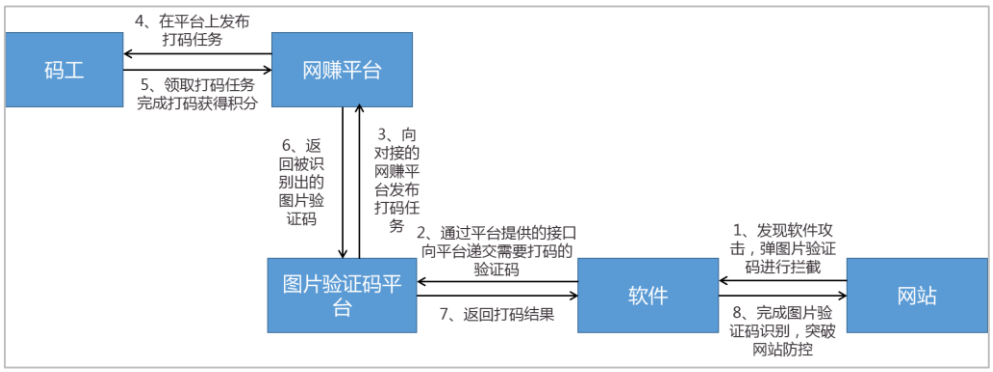

图 4 图片验证码平台的运作链路

打码平台从业人员（码工）主要分布在浙江、广东、河南等区域。

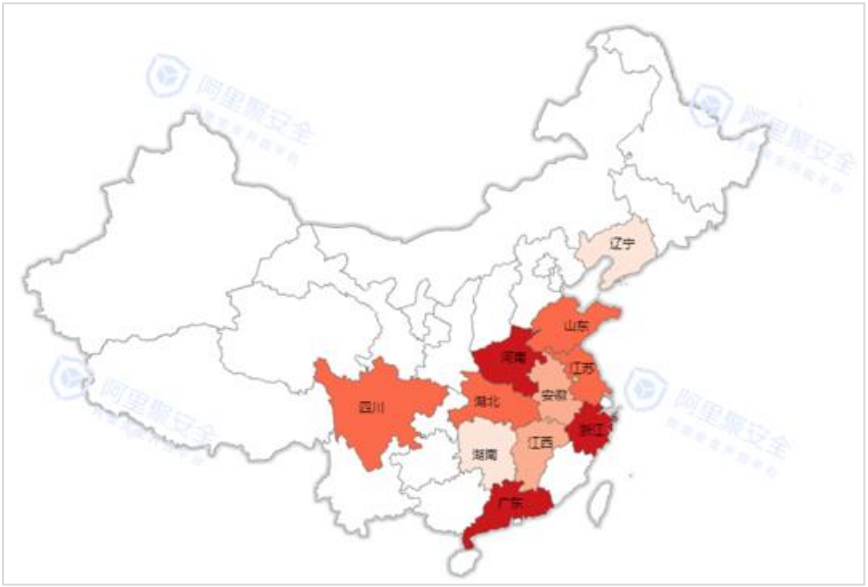

图 5 图片验证码平台的 Top 区域分布

2. 手机验证码平台

手机验证码平台通过整合多方手机验证码商家的资源，作为交易平台衔接验证码卖家与买家。

买家可将手机验证码平台上获得的手机号填入所需注册验证的网站，然后平台就会给买家返回收到的验证码，从而通过网站的验证，一般来说这类手机号是一次性使用。有的网站为了应对以上行为，会对用户的手机号进行反复验证，因此开始有手机验证码平台提供了可长期使用的手机号。一个手机验证码收费从 0.1 元到 3 元不等，相较用实体手机卡成本更为低廉。

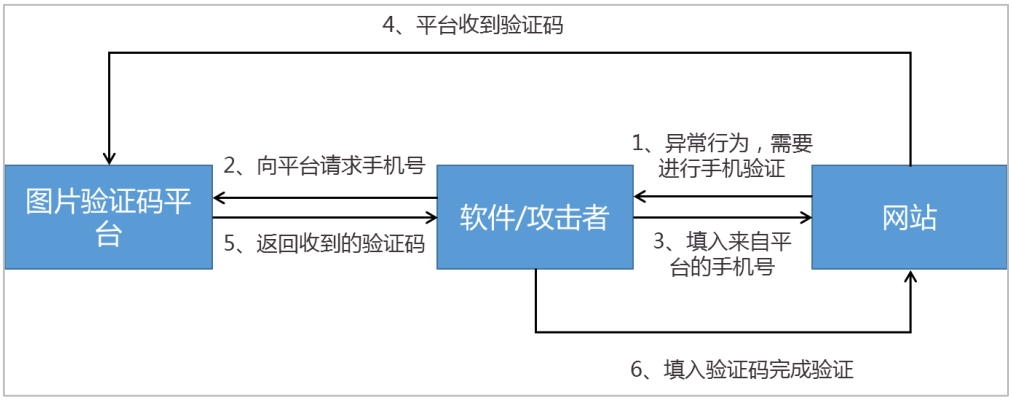

图 6 手机验证码平台的运作链路

手机验证码平台的使用量逐月递增，2015 年平台的充值人数是 2014 年的 3 倍，充值金额是 2014 年的 2.6 倍，涨幅迅猛。

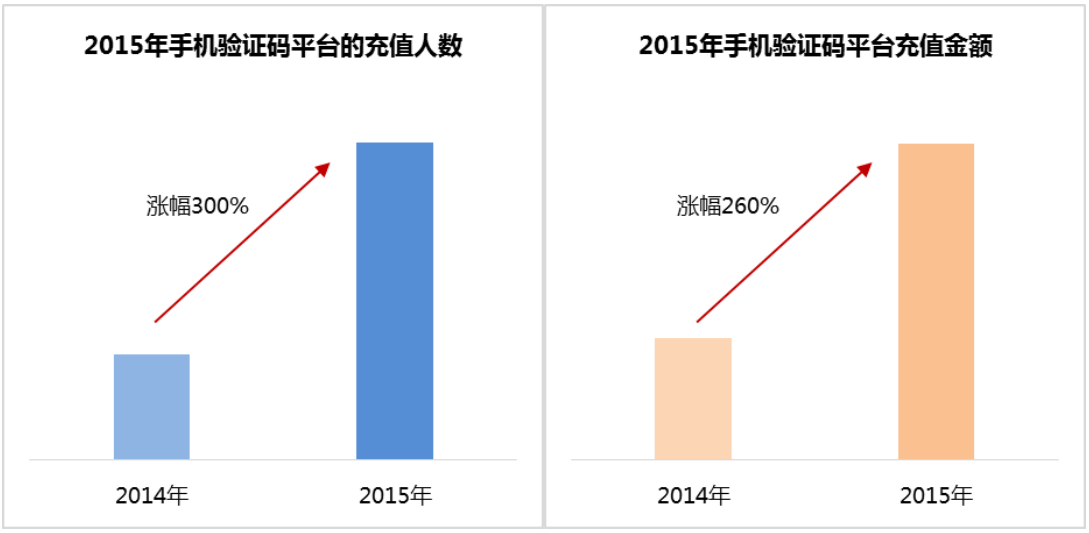

图 7 手机验证码平台充值人数和金额的同比增长

另一方面，手机验证码平台的手机号主要是来源于中国移动、中国联通、中国电信和虚拟运营商，归属地主要是广东、陕西、浙江、河南为主，使用手机验证码平台的人员主要分布在广东、江苏、河南、福建等地。

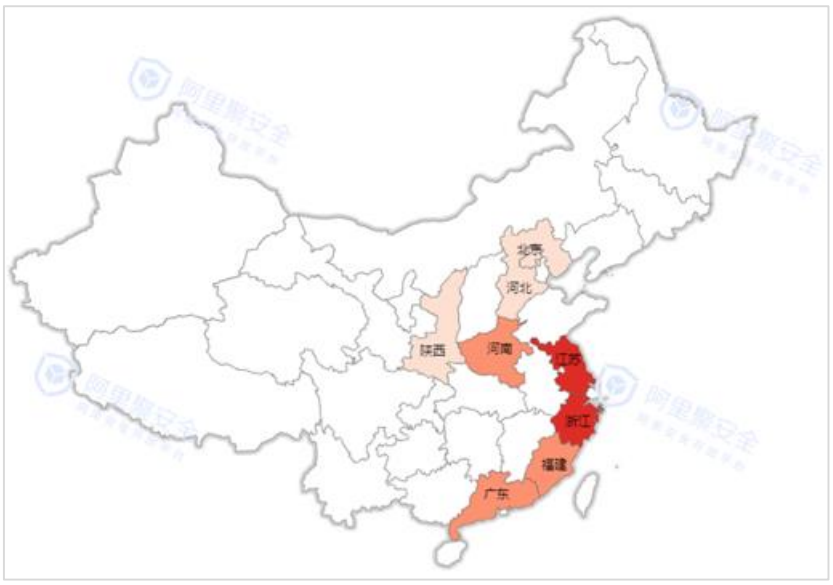

图 8 手机验证码平台的 Top 区域分布

2015 年，手机验证码平台主要用于社交、电商、金融、生活等行业，总占比 88%，这些手机号一半以上都是用于账号注册。

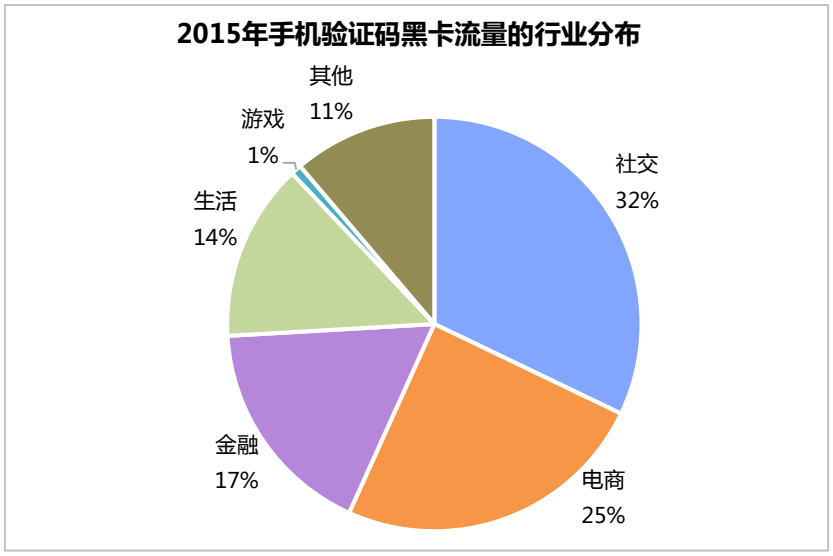

图 9 手机黑卡流向的行业

3. 黑产软件

黑产软件涉猎广泛，包括刷单、盗号、注册、抢购、信息采集、信息群发等，具体制作销售链路如下。

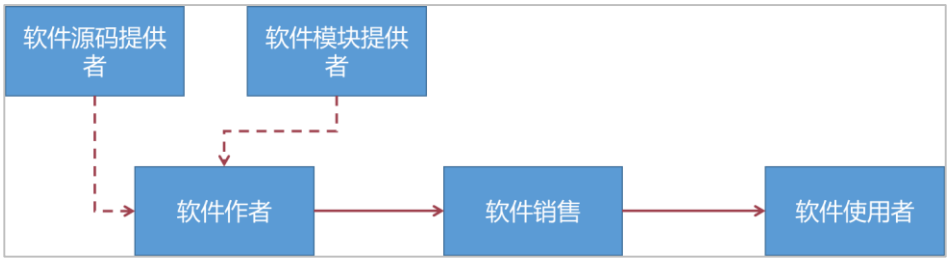

图 10 软件的制作销售链路

2.3 黑产中游：恶意注册、盗号

1. 恶意注册

账号恶意注册是恶意行为的源头，整个流程已趋于专业化、从业人员十万级，形成了手机验证码服务平台、打码平台、注册软件开发团伙、垃圾账号分销平台等一条龙服务。批量性恶意注册主要是通过软件实现的，具体流程如下图。

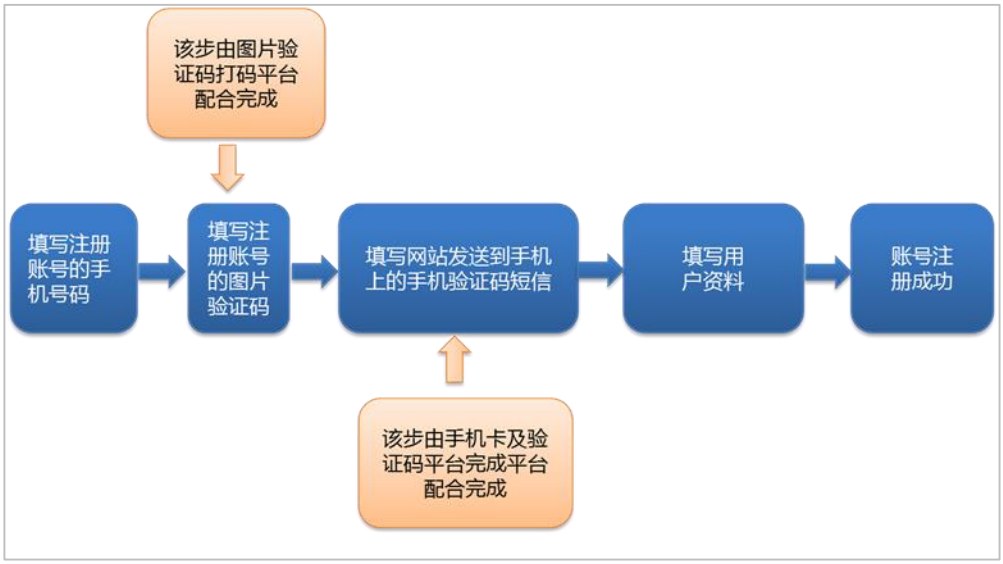

图 11 注册软件批量注册的流程

2. 盗号

黑产在登录环节通过暴力破解、撞库等方式，来获取用户信息进而盗取账号。

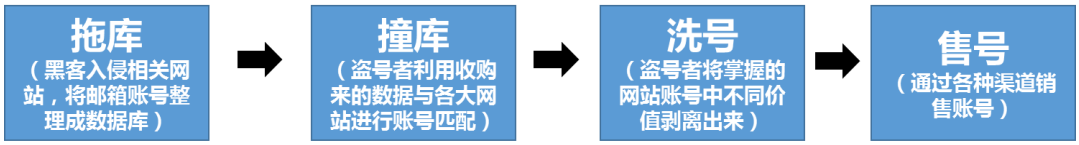

图 12 黑产盗号流程

盗号团伙从黑客手中收购一批拖库而来的账号数据，后将数据与各大 P2P、社交、O2O 等网站进行匹配，通过俗称的“撞库”以获得所需网站的账号密码。盗号团伙掌握网站的账

号密码后通过洗号，剥离有价值的账号，通过各种渠道销售账号获利。

2.4 黑产下游：利益套现

黑产通过上中游的准备，最终将进行利益套现，主要的形式包括活动刷单、欺诈、盗窃、勒索等。

活动刷单是专业团伙通过获取多个账号，使用多个设备，以自动或手动的方式突破平台业务逻辑限制，进行直接谋取暴利的行为。活动刷单是互联网企业在推广时普遍遇到的威胁，主要发生在秒杀、零元购、红包、优惠券等活动中。

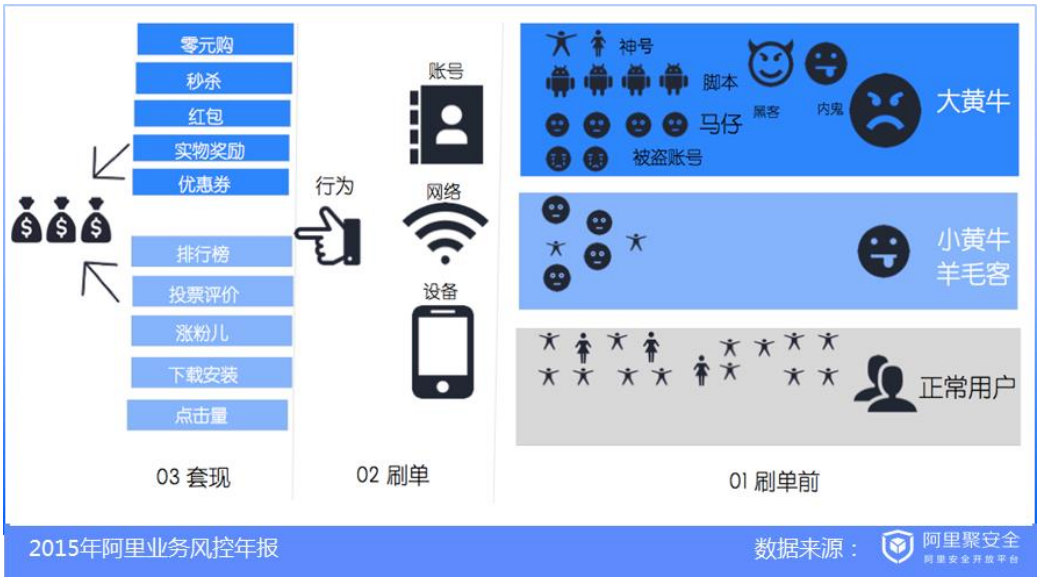

图 13 活动刷单的流程

当今互联网+环境下，刷单现象非常严重、利润率很高，行业分工越来越细，逐渐成为支柱性黑客产业链。其中热门活动被刷的概率达 100%，如某品零元购活动、某知名旅游公司促销红包被刷等案例屡见不鲜，这些被刷的资金直接流入黑产。

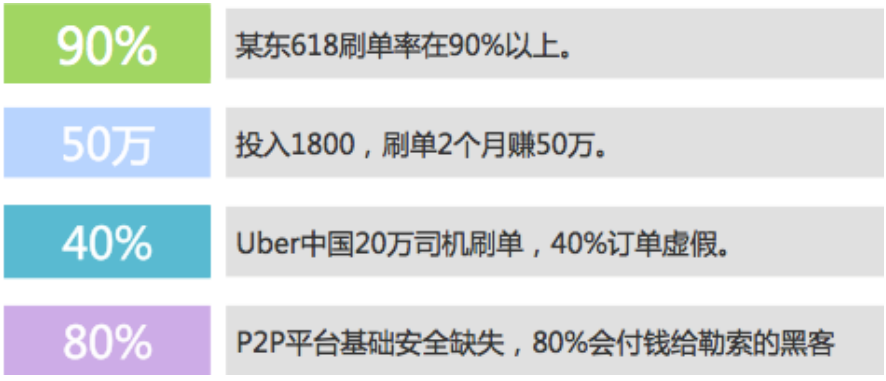

图 14 2015 年部分活动刷单案例

2.5 风险防控方案

虽然整个产业链涉及多个环节，但关键动作均是通过网络账户进行，一般来讲主要涉及三个相互关联的业务场景：

注册场景：大部分网上行为都是基于账号进行，是“黑产”一切活动的基础、弹药，账号量的多少、账号的质量，基本与“黑产团伙”获利成正比，从各平台账号买卖的价格，也可以直接反馈出各平台利益及防控的效果。识别恶意注册，并进行拦截和打击，减少“黑产”能够使用的账号量，可有效减少活动作弊、垃圾消息、欺诈等风险 。

登录场景：登录是一道门槛，通过用户行为及设备特征的分析，大部分的刷库、盗号、活动作弊等风险均可以在登录时识别，提高恶意账号登录门槛，对刷库及被盗风险账号增加相应验证。比如，登录环节通过验证码、短信验证均可降低账号使用风险。在找密、用户信息修改场景也会面临登录相同的风险，可采用相同的防控方法。

活动（交易）场景：这个是“黑产”对抗的主战场，也是减少其获利的直接战场，这里的对抗措施，不能只简单的识别风险，还需要考虑账户的价值，通过机器行为风险与价值双纬度判断，使用身份验证与优惠力度双杠杆调节来使“灰产”无利可图。

2015年，阿里聚安全推出了基于场景的数据风控服务，提供风险评估、风险识别、风险控制的实时防控功能。更多服务介绍和接入，请登录阿里聚安全官网 http://jaq.alibaba.com。

数据风控方案		产品接入方案					
风险场景	服务类型	风险评估	风险识别			风险控制	
			情报数据	机器行为	设备指纹	NC验证码	身份验证
注册	反恶意注册	✓	✓	✓	✓	✓	✓
登录	防被盗、刷库	✓	✓	✓	✓	✓	✓
找密		✓	✓	✓	✓	✓	✓
信息修改	防被盗	✓	✓	✓	✓	✓	✓
活动(交易)	反活动作弊（刷单）	✓	✓	✓	✓	✓	✓

图 15 阿里聚安全数据风控功能

第三章 数据风控发展趋势

账号作为“网络黑色产业链”关键要素，已经可以作为一种攻防效果的衡量指标，账号的买卖价格、账号供应量，可以直接反映出“黑产”规模与被攻击趋势。

基于账户安全的“黑产”已经呈现高回报、高技术、低成本的增长态势，2016年这种趋势将会更具爆发性。

1. “人肉”、“社工”模式规模将扩大

2016年基于业务规则漏洞，采用“人肉”、“社工”方式的恶意组织规模将扩大，恶意注册、账号买卖、盗号、隐私信息买卖、消息推广、刷单、活动作弊等“黑产”各环节均能获利，高回报也将吸引大量人员加入，许多环节已经“人肉”替代了“技术”，风险识别也需要从原来设备、环境更多的向用户行为做综合判断。

2. “实时化”风险识别能力需要增强

2015年，通过与网络犯罪的攻防战，双方响应时间逐渐缩短，从注册一个账号到获利，已经从原来T＋N缩短到分钟级。2016年的对抗将是“实时计算”，实时发现风险、解决风险将是风控系统的发展趋势，由于实时风控系统的建设成本较高，像阿里聚安全这类提供专业实时安全服务的能力将成为主流。

3. “多样化验证”将成为主流

2015 年，大量的账户被盗，已经让用户对于密码失去信心，“去密码”化，将会成为一种趋势，基于风险的“多样化可配置验证”将成为平衡安全与体验的重要手段。

阿里聚安全微信公众号

阿里聚安全官网

阿里聚安全官网：http://jaq.alibaba.com

官方邮箱：mobilesecurity@service.alibaba.com