

真人作弊 黑灰产业研究报告

出品方：鬼谷实验室



了解更多业务情报

目 录

一. 概述与要点	5
二. 发展与现状	6
2.1 多行业、多场景、多任务广泛渗透	6
2.1.1 多行业涉及	6
2.1.2 多场景渗透	7
2.1.3 多任务参与	7
2.2 真人作弊 APP 近年发展迅猛	9
2.2.1 2014 年—2020 年 APP 活跃量及下载量指数级增长 ..	9
2.2.2 2014 年—2020 年开发者增长迅速	11
2.3 真人作弊参与人群画像	13
2.3.1 真人作弊产业人数	13
2.3.2 真人作弊男女比例	14
2.3.3 真人作弊年龄分布	14
2.3.4 真人作弊参与人数地域分布	15
2.4 真人作弊对行业造成的损失统计	15
三. 痛点与危害	17
3.1 真人作弊 vs 机器作弊	17
3.2 真人作弊 vs 传统风控	17

3.3 真人作弊带来的额外风险	18
四. 对抗与解决	20
4.1 情报维度	20
4.2 数据维度	20
五. 写在最后	22



永安在线
EverSafe Online

版权声明

本报告版权归深圳永安在线科技有限公司所有，并受相关法律法规保护。未经允许不得擅自转载、摘编或利用其他形式使用本报告文字或观点。如需转载请联络永安在线。违反上述声明者，将追究其相关法律责任。



永安在线
EverSafe Online

一. 概述与要点

真人作弊俨然已经发展成为目前黑灰产最常见、最难以防御、同时也对风控体系破坏极大的一种侵害平台整体安全性及稳定性的作恶形式，在隐秘的角落里，它无时无刻不给平台带来伤害。永安在线基于长期对真人作弊产业的调查和研究，深入剖析这个产业的方方面面，解析真人作弊产业的发展、现状、危害以及防御思路，力求以最专业、最全面的视角呈现它的全然样貌。

本次研究报告的要点如下：

- 1) 真人作弊黑灰产经过数年发展，模式和形态越发多元和丰富，已渗透至众多场景、众多行业；
- 2) 真人作弊黑灰产发展迅猛，自 2014 年至 2020 年，真人作弊平台（app）的数量在增长了近 40 倍，参与人数增长了近百倍；
- 3) 相较于机器作弊，真人作弊对甲方的风控和安全能力提出了更高的要求，带来了新的挑战；
- 4) 以情报能力和数据能力为风控赋能，是识别新型欺诈模式的有效方式方法。

二. 发展与现状

本质上，真人作弊源于人的贪婪和惰性，驱动因素是互联网技术和企业与黑灰产长期攻防对抗，从而演化出了此类比较高级的作恶形态。近年来，这种模式和形态越发多元和丰富，从早期单一的兼职刷单，到如今的多行业、多场景、多任务的广泛渗透；从早期的只在 PC 端进行的单一手法的兼职，到如今以移动端为主；从早期的线上群组媒介（QQ 群、YY 语音等），到如今平台化、裂变化。

2.1 多行业、多场景、多任务广泛渗透

2.1.1 多行业涉及

真人作弊涉及的行业极其广泛，从金融领域到 UGC 娱乐，从生活服务、视频音频到新闻资讯、社交聊天等，无所不涉。如下图所示，是真人作弊的目标行业类型占比：

真人作弊目标行业类型占比

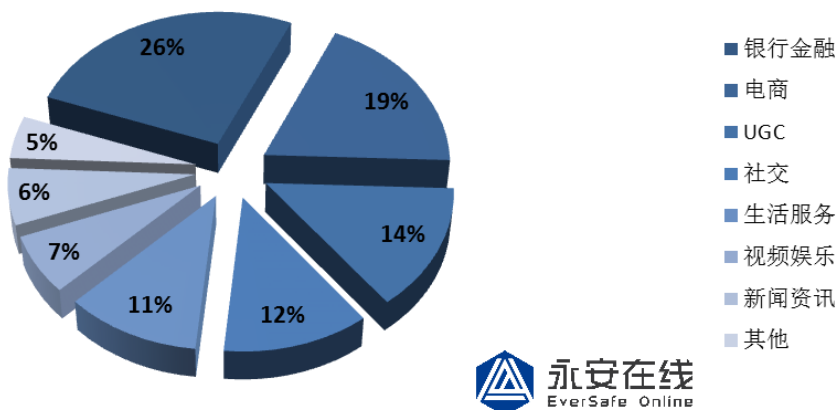
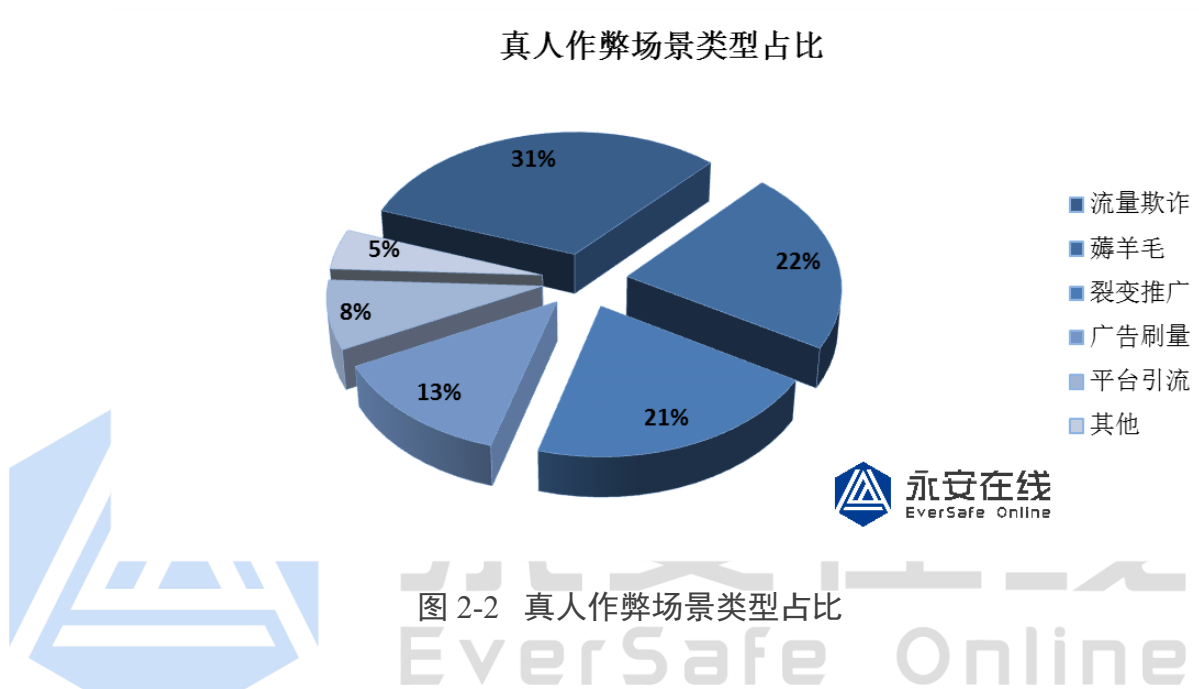


图 2-1 真人作弊目标行业类型占比

2.1.2 多场景渗透

在业务范围方面，真人作弊也几乎涵盖了所有黑灰产作恶场景，无论是薅羊毛、流量欺诈，还是广告刷量、平台引流、裂变推广等场景，真人作弊都参与其中。具体占比见下图：



2.1.3 多任务参与

真人作弊任务，同样是包罗万象，你能想到的所有可以赚取利润的任务，都被真人作弊染指：下载注册、认证绑卡、评论关注、助力砍价、阅读分享、投票转发等无一不包，具体占比见下图：

真人作弊任务类型占比

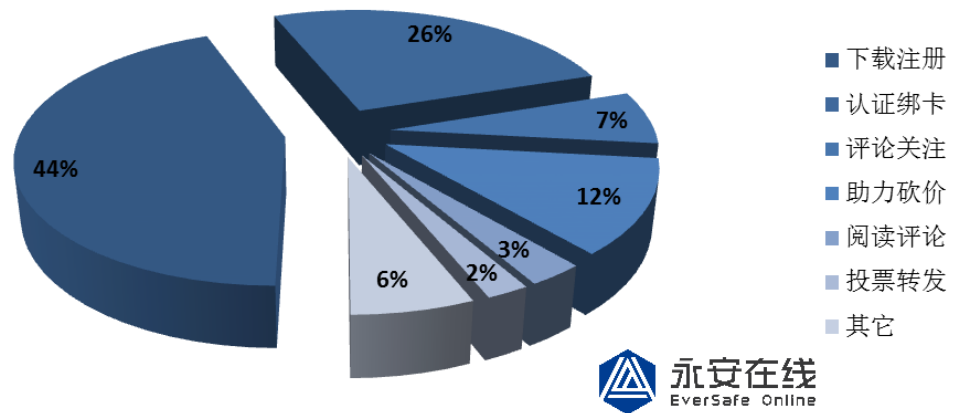


图 2-3 真人作弊任务类型占比

通过统计长期监控到的真人作弊任务标题、内容和关键词,形成以下词云图,从中也可看出真人作弊的主要关注任务是:下载注册、认证绑卡、评论关注等。



永安在线
EverSafe Online



图 2-4 真人作弊任务类型词云图

2.2 真人作弊 APP 近年发展迅猛

2.2.1 2014 年—2020 年 APP 活跃量及下载量指数级增长

在最早期，真人作弊还是以“线上群组”的方式为媒介进行交流和信息传播，典型的有 YY 语音群组、QQ 黑灰产交流群、论坛聊天等，但是当互联网走向移动化之后，真人作弊也紧跟时代发展的步伐。

永安在线监控到，从 2014 年到 2020 年，真人作弊 APP 数量呈现几何式增

长：2014 年的时候不到百款，到今年近三千款，如下图所示：

2014年—2020年真人作弊APP活跃数量发展走势

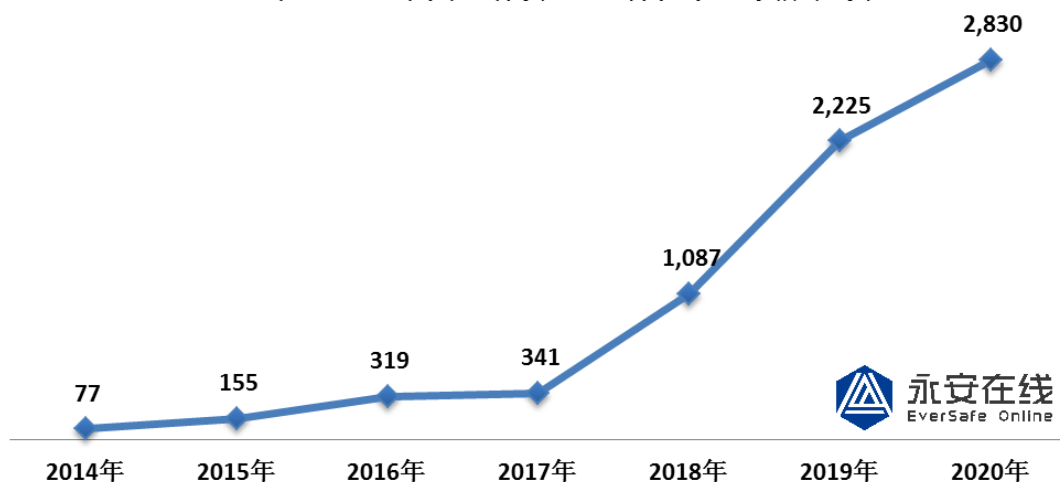


图 2-5 2014 年—2020 年真人作弊 APP 活跃数量发展走势

（注：2020 年上半年整真人作弊 APP 的活跃数量为 1,415 款，基于 2019 年的数量，以及真人作弊的发展现状，我们合理推测：2020 全年活跃的真人作弊 APP 可达 2,830 款。）

在真人作弊 APP 活跃数量呈几何式增长的时候，相关的下载量也增长迅猛：

2014年—2020年真人作弊APP下载数量发展走势

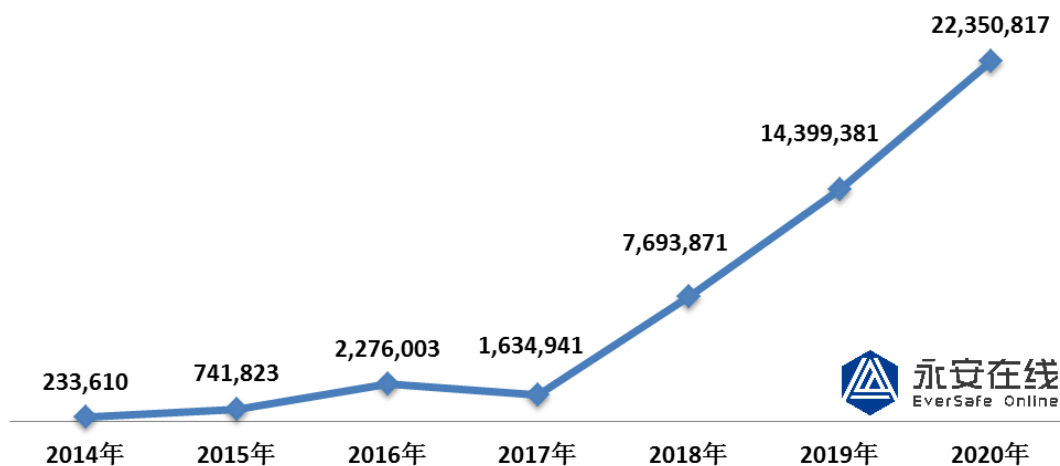


图 2-6 2014 年—2020 年真人作弊 APP 下载数量发展走势

（注：2020 年上半年整监测到的真人作弊 APP 下载量为 12,350,817 次，基于 2019 年的下载数量，以及真人作弊的发展现状，我们合理推测：2020 下半年

版权所有：深圳永安在线科技有限公司

真人作弊 APP 的下载量可以再增加 10,000,000 次，最终至全年下载量为：22,350,817 次。）

2.2.2 2014 年—2020 年开发者增长迅速

真人作弊参与人数爆发式增长的背后，离不开资源的支撑，其中一个重要资源就是平台：真人作弊平台——即真人作弊 APP，这一方面可以从真人作弊 APP 的开发者数量中体现，在永安在线监控到的数据中，我们可以发现真人作弊 APP 的开发者数量同样呈现指数形式的增长：从 2014 年的不足 20 个，到今年的 1500 左右，发展速度惊人。

2014 年—2020 年真人作弊 APP 开发者数量发展走势

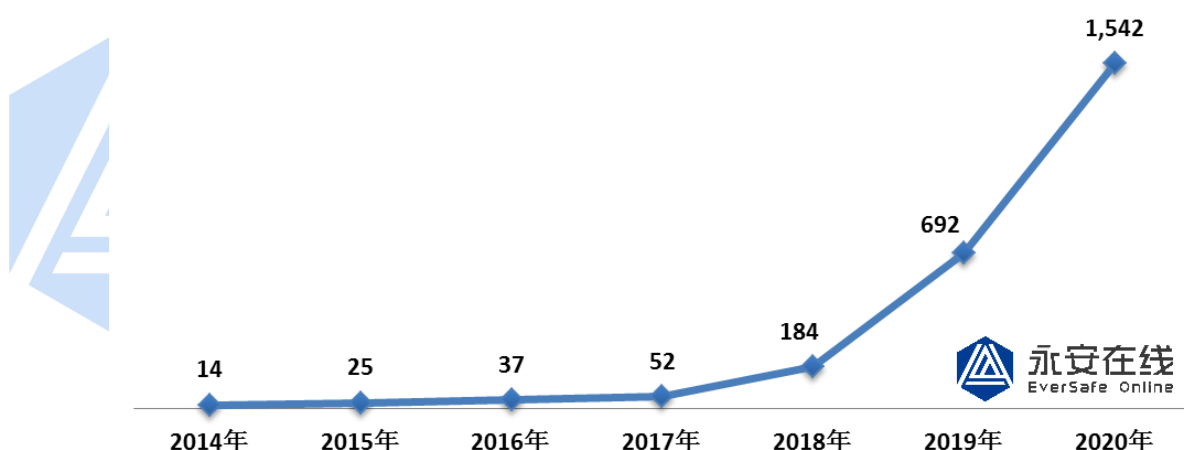


图 2-7 2014 年—2020 年真人作弊 APP 开发者数量发展走势

（注：2020 年上半年整监测到的真人作弊 APP 开发者数量数量是 771 个，基于真人作弊发展现状，我们合理推测：2020 年全年真人作弊 APP 开发者数量可达到 1,542 个。）

在永安在线监控到的所有移动开发者中，企业开发者有 1,407 个，占比总数 1,598 的 88%。

各类开发者数量占比

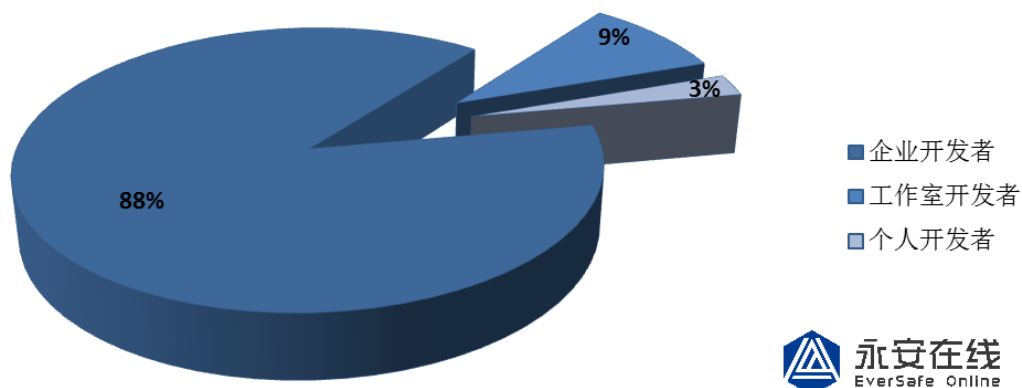


图 2-8 各类型开发者数量占比

企业开发者占比近 90%，提供真人作弊平台类服务的利润可见一斑。因小知大，这也从侧面反映出，整个真人作弊产业的利润何其丰厚。

开发者的地域分布也和中国互联网的地域发展特征基本吻合，前四个地区分布是：北京、上海、深圳、杭州：

真人作弊开发者城市分布

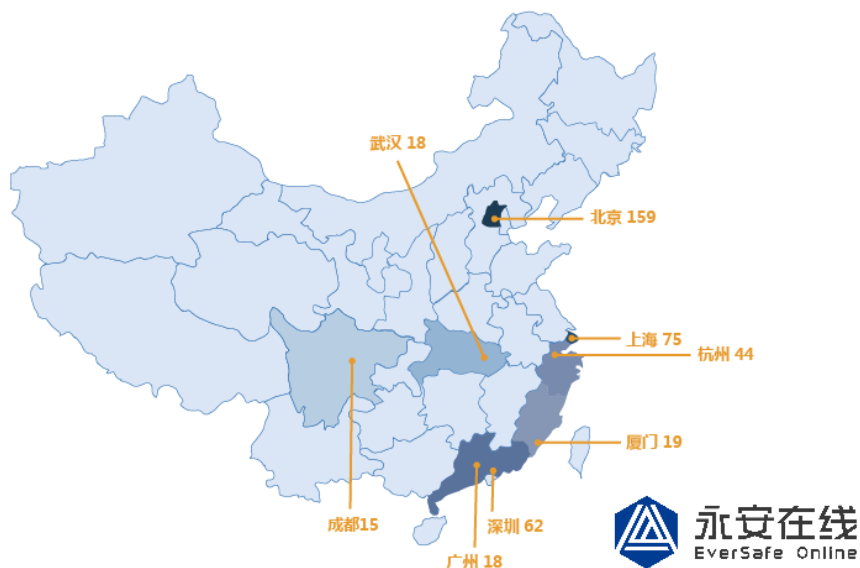


图 2-9 真人作弊开发者城市分布

更有甚者，个别公司同时开发了很多款真人作弊平台了 APP，比如位于蚌埠的某家公司，同时开发了 23 款真人作弊 APP；青岛的某家公司，同时开发了 10 款真人作弊 APP 等等。所谓无利不起早，可见开发真人作弊 APP，能够为这些公司带来的利润不会太少。

2.3 真人作弊参与人群画像

那么，参与真人作弊的用户都有什么特征呢？请看以下画像描述。

2.3.1 真人作弊产业人数

任何一个产业的兴起，都离不开人的参与。如上所见，无论是真人作弊任务的多样性还是 APP 的蓬勃发展，其背后都是因为巨大的需求推动。实际上，永安在线监控到的参与真人作弊的用户的确呈现指数型增长，从 2014 年的十万余人，到今年的保守估计约一千一百万，七年翻了百余倍，“真人作弊的力量”已不容小觑：

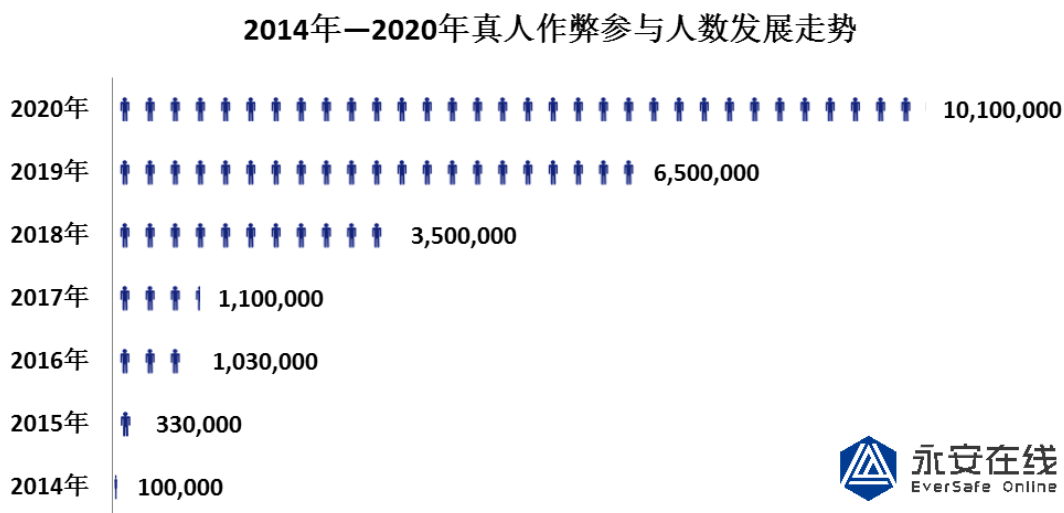


图 2-10 真人作弊参与人数发展走势

2.3.2 真人作弊男女比例

通过对参与真人作弊用户群体的随机抽样调查发现，真人作弊参与者以男性居多，占比为 64%，女性为 36%：

真人作弊参与者男女比例

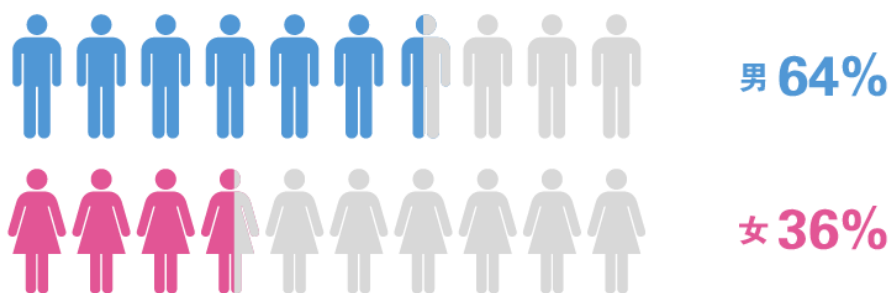


图 2-11 真人作弊参与者男女比例

2.3.3 真人作弊年龄分布

在年龄分布方面，90 后是真人作弊的主力军，占比 45%，接下来是 00 后及 80 后，分别占 21%和 15%，可见参与作弊的人普遍年轻，这也从侧面反映出来，真人作弊的产业还会继续发展下去。

真人作弊参与者年龄分布

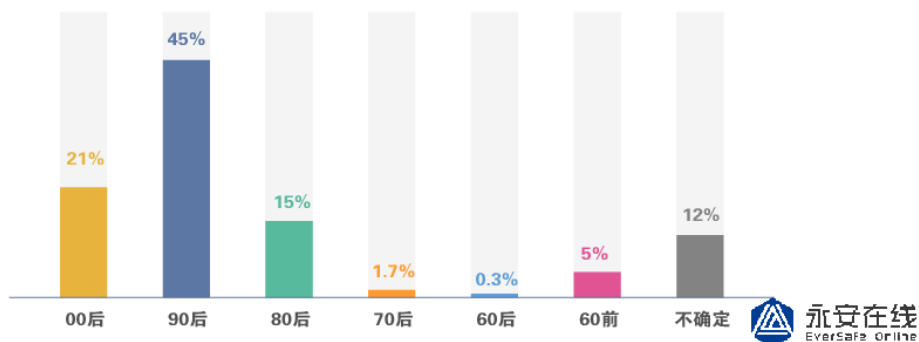


图 2-12 真人作弊参与者年龄分布

版权所有：深圳永安在线科技有限公司

2.3.4 真人作弊参与人数地域分布

从地域上来看，真人作弊的参与者分布在华南、华东、华北、华中这几个区域，其中华南区域的广东省占比最多，达 35%：

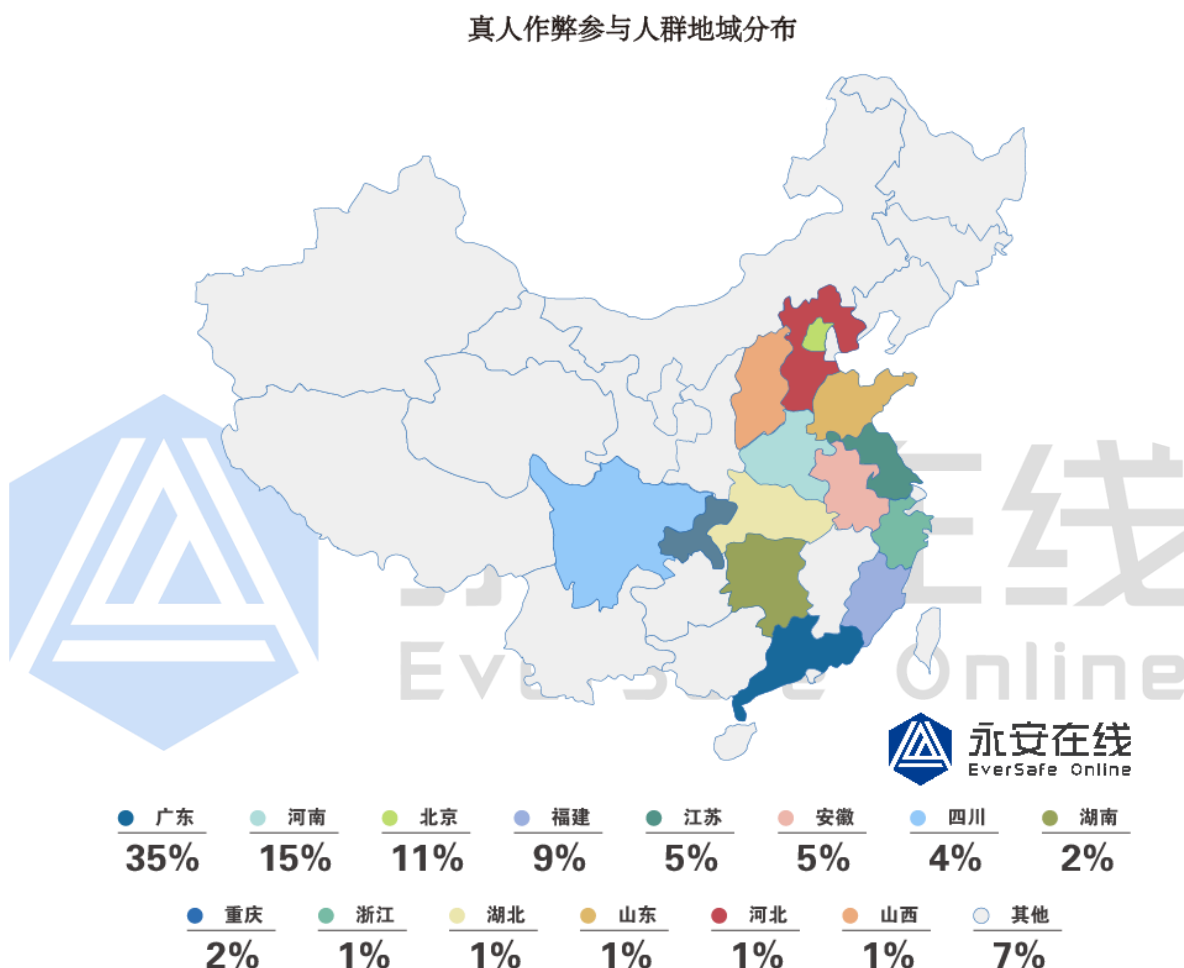


图 2-13 真人作弊参与人群地域分布

2.4 真人作弊对行业造成的损失统计

那么真人作弊对各个行业造成的损失是多少呢？

永安在线对近半年的真人作弊平台任务进行了全量统计，以悬赏数量、悬赏

金额、完成数、悬赏时间、完成时间等因素进行计算，共得出以下结论：

真人作弊产业每年约产生 20 亿元的悬赏金额流水、10 亿元完成金额流水，直接对目标平台造成数十亿甚至百亿的损失。



永安在线
EverSafe Online

三. 痛点与危害

3.1 真人作弊 vs 机器作弊

	真人作弊	机器作弊
作恶群体	黑产团伙+大量真实用户	黑产团伙
作恶设备	真机	群控、云手机、模拟器
作恶资源	真实手机号、真实IP	黑卡、黑IP
作恶流程	真人操作	协议破解/模拟操作

表 3-1 真人作弊和机器作弊特点对比

3.2 真人作弊 vs 传统风控

传统风控是基于黑产资源和黑产团伙所表现出的“非正常人”的特征来做风险行为的检测和识别，当黑产藏匿于幕后，以现金奖励调动真实用户完成作弊任务，“人机识别”被“真人”挑战，传统风控便显得捉襟见肘。风控痛点具体表现在以下四个方面：

1) 防护手段失效

无论是规则层面的风险数据库、风险规则库、风险特征库等，还是模型层面的 AI 算法、决策引擎等，其知识的积累主要来自于长期对机器作弊的数据分析与沉淀。猫池黑卡、代理 IP 等传统风控数据黑名单完全不适用于真人作弊的场景，另外，真人作弊人群行为、画像、用户关系等特征往往比较离散，且变化多样，虽然不是完全的无迹可寻，但算法模型的输入强依赖于安全人员对风险数据和场景的洞察和分析能力，需要非常高的运营成本。

2) 处置边界模糊

相较于处置违规的黑产账号，处置违规真实用户账号的复杂度大幅提升。如何合理地对真实用户的违规行为分类分级，如何兼容风控指标和用户体验，如何向业务团队提供强可解释性的处置理由等等，这些对于风控团队而言，考验进一

步升级。

3) 风险响应滞后

一旦真人作弊风险事件发生，在前期风控团队几乎是无力的，只能任风险事件的影响范围不断扩大。从风险事件的发生，到对抗方案的实施落地，时间差越大，损失越大。真人作弊场景下，这个时间差远大于机器作弊。

4) 溯源复盘困难

真实用户介于黑产与受害企业之间，为黑产筑起天然屏障，难以进行事后追踪与溯源。且从已掌握的作弊数据，只能关联扩散有限范围的作弊数据，真人作弊模式变化频繁，无法对今后的真人作弊行为形成有效的知识传递与经验复用。

3.3 真人作弊带来的额外风险

除了常见的机器作弊带来的常见危害（如营销作弊、渠道作弊、虚假用户、刷单假量等）之外，真人作弊还引入了个人信息被黑产滥用和泄露的风险。

黑产收购真人用户注册的账号，用于不法用途。黑产诱导真人用户协助完成好友辅助认证、实名、人脸认证等，真人用户不但违反平台用户条款，甚至还需承担潜在的法律风险。

另外，永安在线安全团队在对真人作弊产业链进行调查的时候，曾经深入调查一个金融类的悬赏任务，这个任务是“认证绑卡”类型的任务：用户只需要绑卡成功就能得到 30—50 元的佣金奖赏。

首先，从收入产出比上看，黑产肯拿出这么高的佣金，说明黑产的收益很可能达到百元甚至更多，所以对于进行推广的金融平台来说，必然会承受不小的损失；其次，我们在与任务发布者进行聊天的时候，被要求在完成任务后提供：姓名+手机号+身份证+银行，如下图所示：

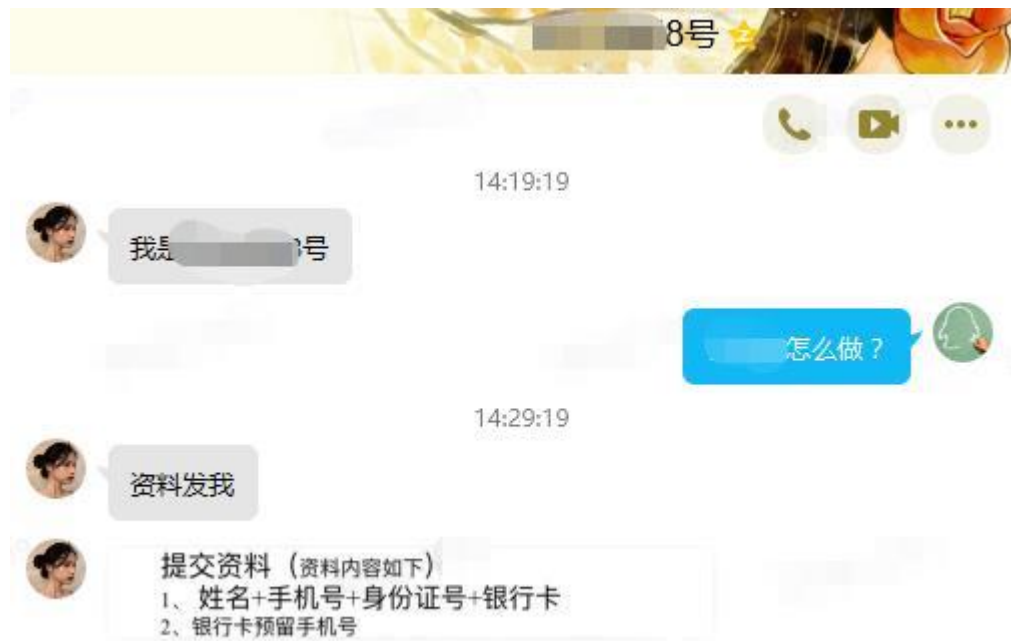


图 3-与任务发布者聊天

注意，把这些资料交给任务发布者之后，还是不能拿到佣金，必须完成最后一步：把手机接到的短信验证码交给任务发布者后，才能收到佣金。姓名、手机号、身份证、银行卡以及短信验证码，是非常敏感的个人信息，完全暴露在黑产的控制之下，个人信息甚至财产安全受到严重威胁。

四. 对抗与解决

如此澎湃汹涌的真人作弊，有着相对于机器薅羊毛的种种优势，以及对传统风控直捣黄龙式的挑战，所带来的挑战愈发严峻。那么，到底该怎么防控呢？

永安在线认为，情报能力和数据能力为风控赋能，是对真人作弊新型欺诈模式的解决办法。

4.1 情报维度

举个例子，永安在线去年在对真人作弊平台进行全面监控的时候，发现了一些类似这样信息的任务：

“注册下载 XX 软件，密码统一设置为 a123456，做完之后与我联系结付。”

之后，我们顺藤摸瓜，在其余的几百个真人作弊平台中找到了同类相关任务达近十万个，其密码设置要求都是一样的，这明显说明是同一个团伙在对这个平台进行批量注册类攻击，为了便于记忆和统一管理，所以要求任务完成者设置统一的简单密码。

我们捕捉到这个威胁信息之后，进行了全网的情报搜集和关键信息整理，包括密码特征、任务发布者信息、任务最早开始时间等等，然后第一时间把这些关键信息交给了该社交平台。平台在接到我们的情报信息之后，也在第一时间进行了反向溯源和定位，结果的确揪出来了一个大型的灰产团伙，并成功打击，直接维护了平台的安全、和谐，并提前将伤害扼杀在摇篮之中。

4.2 数据维度

情报维度的信息，可以帮助我们直接抹去和黑产之间的信息差，并在最短的时间夺取主动权，然而，仅有情报信息，终究单薄，此时还需要数据信息对黑产进行定位以及后续挖掘工作的支持。真人作弊相关的风险数据包括：风险 APP、风险设备、风险账号以及真人作弊中任务的二维码、链接、教程、任务流程等等。

举个例子，今年 5 月份开始，某家国内支付平台开始作拉新和绑卡送礼的活

版权所有：深圳永安在线科技有限公司

动，因为涉及到支付和银行卡，所以奖励金额很高，这自然会被黑灰产盯上。但毕竟这类活动要求实名、绑定银行卡等，机器作弊的成本和门槛较高，所以拥有特定渠道资源的黑灰产开始在众多真人作弊平台发布任务（我们在长期跟踪研究之后发现，有些黑灰产团伙拥有大量的返现资源，这种资源被他们成为“口子“）。

永安在线在第一时间感知到威胁之后，对此类作弊方式进行了重点监控，一方面从情报维度进行广泛的情报收集与分析，一方面基于永安在线上亿级的设备画像能力，对真人作弊用户进行了风险设备的定位以及信息提取工作，另外也把这些风险设备、任务分享链接和结算链接等数据特征交付给了该支付平台。

平台在收到数据后进行了匹配验证，直接发现了数千个风险账号，之后又通过这些账号的共性行为和网络关系再次定位到了数百个上游师傅账号，以及数万个下游风险账号。永安在线进一步协助该平台研究这些师傅账号的行为，发现这些师傅账号长期隐匿在平台，每逢活动就组织薅取羊毛的恶意用户。



五. 写在最后

当企业绞尽脑汁、苦思冥想对付黑灰产的时候，黑灰产总能找到企业的安全短板，攫取利益；当企业自以为终于跟上黑灰产的脚步，暗想可以把黑灰产防守在门外的时候，其实只是看到了黑灰产的后脚跟；当企业 360 度防护、采用了各种高级的规则算法模型的时候，黑灰产开始“返璞归真”，采用最朴实的真人作弊方式对抗最先进的技术。风控路漫漫，安全无松懈，面对不断进化的黑灰产，单纯的技术攻防将左支右绌，唯有及时跟进黑灰产的步伐，才不至于太过于被动。



永安在线
EverSafe Online

说 明

1. 数据来源说明：

本报告数据来源于永安在线旗下 Karma 业务情报搜索引擎，基于 Karma 上监测到的数据进行取样分析，所得的数据分析结果与实际情况之间可能存在一定的偏差，敬请谅解。

2. 业务情报监测平台说明：

业务情报监测平台 Karma，以攻击者的视角，依托强大的黑灰产布控能力及深层次的情报处理能力，帮助企业在业务环节精准筛选出恶意流量，还原风险场景，并量化对业务的影响，且持续对黑产进行实时监测，驱动风控决策引擎迭代，从而提升企业整体攻防效率。



永安在线
EverSafe Online