联合发布单位：

腾讯游戏安全 | 腾讯安全 | 伽马数据 GAMMA DATA | DataEye

指导单位：

广东省游戏产业协会

2024

游戏安全白皮书

2024 Game security White Paper

CONTENTS

01 PART

02 PART

03 PART

04 PART

05 PART

06 PART

07 PART

08 PART

09 PART

前言
PREFACE

在全球数字经济与游戏产业深度融合的进程中，中国游戏行业持续释放创新活力，跨平台技术革新与全球化战略的推进为产业发展注入新动能，根据《2024年中国游戏产业报告》，2024年，中国游戏市场实际销售收入为3257.83亿元，同比增长7.53%，游戏用户规模6.74亿人，同比增长0.94%，为历史新高点。

然而，产业繁荣的背后，游戏安全威胁正以更专业而隐匿的形态侵蚀生态根基——从传统外挂黑产的持续进化，到内容安全的跨境挑战，多维度的风险交织对行业提出前所未有的考验。面对复杂的安全态势，防御体系正经历从被动响应到主动治理的范式升级。在这个全新的游戏产业发展大环境下，**在广东省游戏产业协会的指导下，腾讯游戏安全联合腾讯安全、伽马数据、DataEye编撰了《2024游戏安全白皮书》**，旨在为游戏产业的安全发展提供全面的参考和指导。

今年是**腾讯游戏安全团队成立20周年，作为广东省游戏产业协会游戏安全专委会的主任委员单位，**腾讯游戏安全这20年来，在游戏安全领域深耕，已经总结出一套较为完善的安全对抗体系，本白皮书将与行业分享在游戏安全对抗中的各类实战经验。

同时，今年也是我们**连续第四年发布游戏安全白皮书**，基于对行业安全生态的长期观察，本白皮书系统梳理了游戏外挂、经济安全、内容安全、账号安全等核心议题，同时，还盘点了我国在游戏安全上的法律法规，以及行业共建的重要事件和成果。

在未来的趋势中，游戏安全将越来越与AI、大数据、云计算等领域深度结合，需要全球游戏厂商联合起来，构筑更加具有强大防御能力的智能安全体系。在这个蓬勃发展和充满挑战的时代，我们期待与广大业内人士携手、共同捍卫、推动游戏行业的健康发展，保障游戏玩家的公平竞技。

连续 **4** 年
发布游戏安全白皮书

腾讯游戏安全团队成立
20 周年

游戏面临的安全风险与挑战

GAMING SECURITY RISKS & CHALLENGES

02.

据腾讯游戏安全一项覆盖18个省份玩家和30个游戏厂商的调研显示，游戏外挂问题严重是玩家放弃一款游戏的重要原因之一，超过85%的玩家认为游戏安全对游戏非常重要，55%的玩家认为若弃游后，只要游戏解决了外挂问题，都愿意回流该游戏。

而对游戏厂商而言，30家被访厂商均表示对自己的游戏安全环境非常重视，大部分被访游戏厂商表示都在使用游戏安全产品，个别厂商自建安全团队的同时，也通过与业内安全服务提供商合作，打造游戏安全防护体系。

由此可见，无论是对于玩家或者游戏厂商，游戏安全问题已持续成为最受关注的问题之一，安全问题成为全体游戏人不得不跨越的一座大山。

不同游戏品类所面临的游戏安全问题会有所不同 ，游戏厂商应根据自身的游戏品类，制定相应的安全策略和方案。

	动作射击游戏类 (STG)	多人在线竞技游戏类 (MOBA)	角色扮演游戏类 (MMORPG)	策略游戏类 (SLG)	休闲游戏类 (Casual Game)
外挂	★★★★★	★★★★	★★★★	★★★	★★★★★
打金工作室	★	☆	★★★★★	★★★★	★★
违规内容信息	★★★	★★★★★	★★★	★★	★★★★
消极游戏行为	★	★★★	☆	☆	☆
账号安全	★★★★	★★★★	★★★★★	★★★	★★★★
演员	★	★★	☆	☆	☆
代练	★	★★★	★	☆	☆

备注：★ 越多表示面临的挑战越大，同时，游戏日活跃量越大，上述问题的严重性会更加突出

01. 外挂问题

游戏外挂指的是通过读写游戏数据获取不正当利益的作弊程序或软件。游戏外挂可以通过读写或修改游戏数据、游戏代码、游戏协议，破解游戏客户端，使用第三方辅助插件等手段，实现自动操作、视角修改、无视游戏物理规则、获取视野等效果，获得竞争或资源上的优势，破坏游戏公平性。

游戏外挂的类型

按照外挂的制作类型，从大类上来分，通常将外挂分成**通用外挂**和**定制外挂**两大类。两者的核心区别主要是看外挂是否需要针对特定的游戏进行定制适配和开发。

通用外挂通常不需要结合游戏逻辑、无需额外的游戏适配和开发，通过软件和硬件技术来实现各类外挂功能。

定制外挂通常需要结合游戏逻辑，进行额外的游戏适配和开发，如资源、协议以及内存的获取和攻击来实现外挂功能。

另外，把通用外挂和定制外挂，按照外挂功能来分类，可以分成以下**细分种类**。

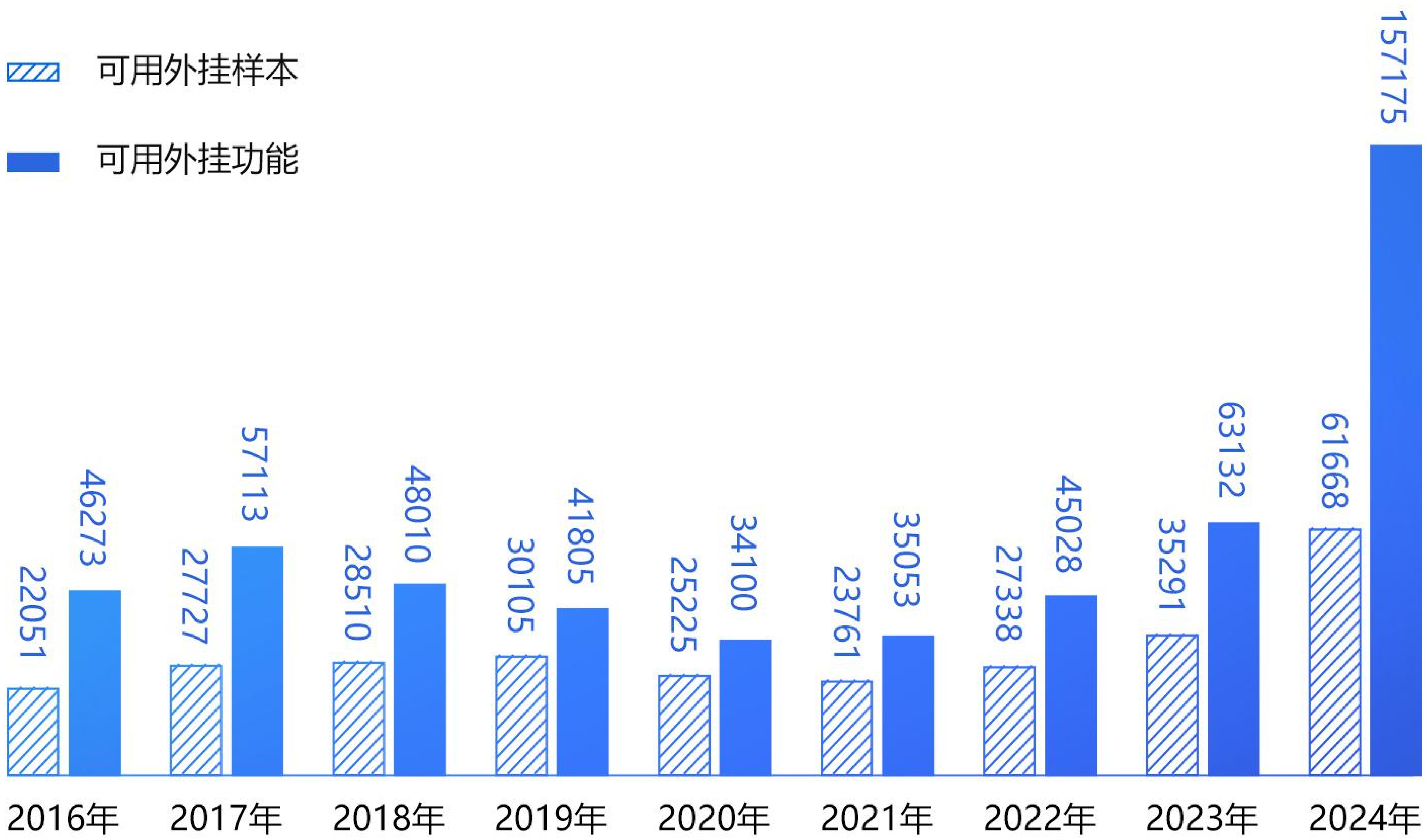
通用外挂
定制外挂
> **核心区别** > **外挂是否需要针对特定游戏进行定制适配和开发**

通用外挂		定制外挂			
不针对一款或一类游戏 不需要特适配和开发的外挂		针对一款或一类游戏 需要特定游戏适配和开发的外挂			
通用软件挂	**通用硬件挂**	**模拟挂**	**内存挂**	**协议挂**	**资源挂**
变速器	同步器	挂机脚本	倍攻挂	脱机挂	换肤挂
打码工具	分屏器	AI外挂	透视挂	封包工具	
机器码修改器	Kmbox	按键精灵	加速挂	DDoS挂	
修改器	DMA硬件	鼠标宏			
		机械臂			

PC端游戏的外挂问题

2024年，受新的射击类强竞技游戏款数和玩家规模持续增加，带动黑产关注度，腾讯PC游戏的外挂对抗的外挂样本数及功能数都有明显增长。2024年检测到的外挂样本达到61668款，同比2023年的35291款增长74%。而外挂功能数达到了157175款，同比2023年的63132款增长149%。

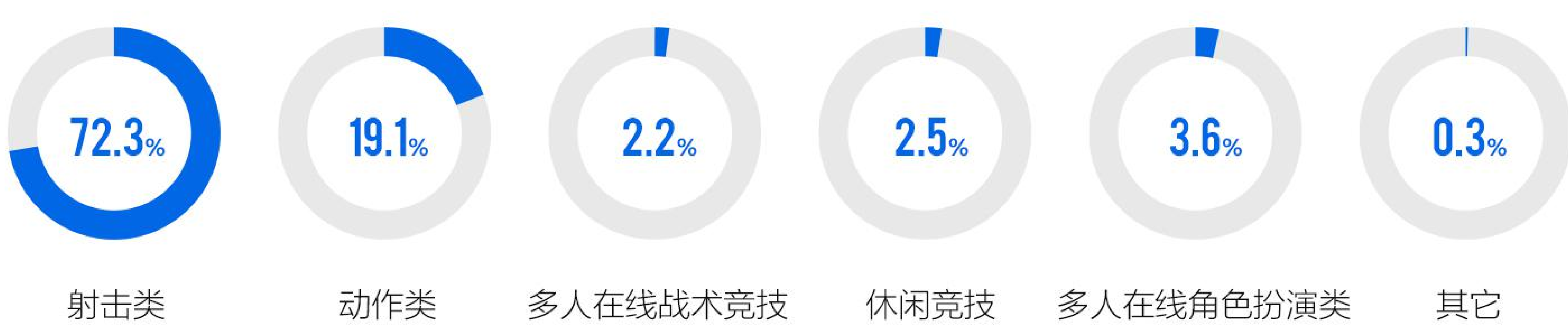
腾讯PC端游戏近年来对抗的外挂样本数及功能数



射击类游戏、动作类游戏外挂问题最严重

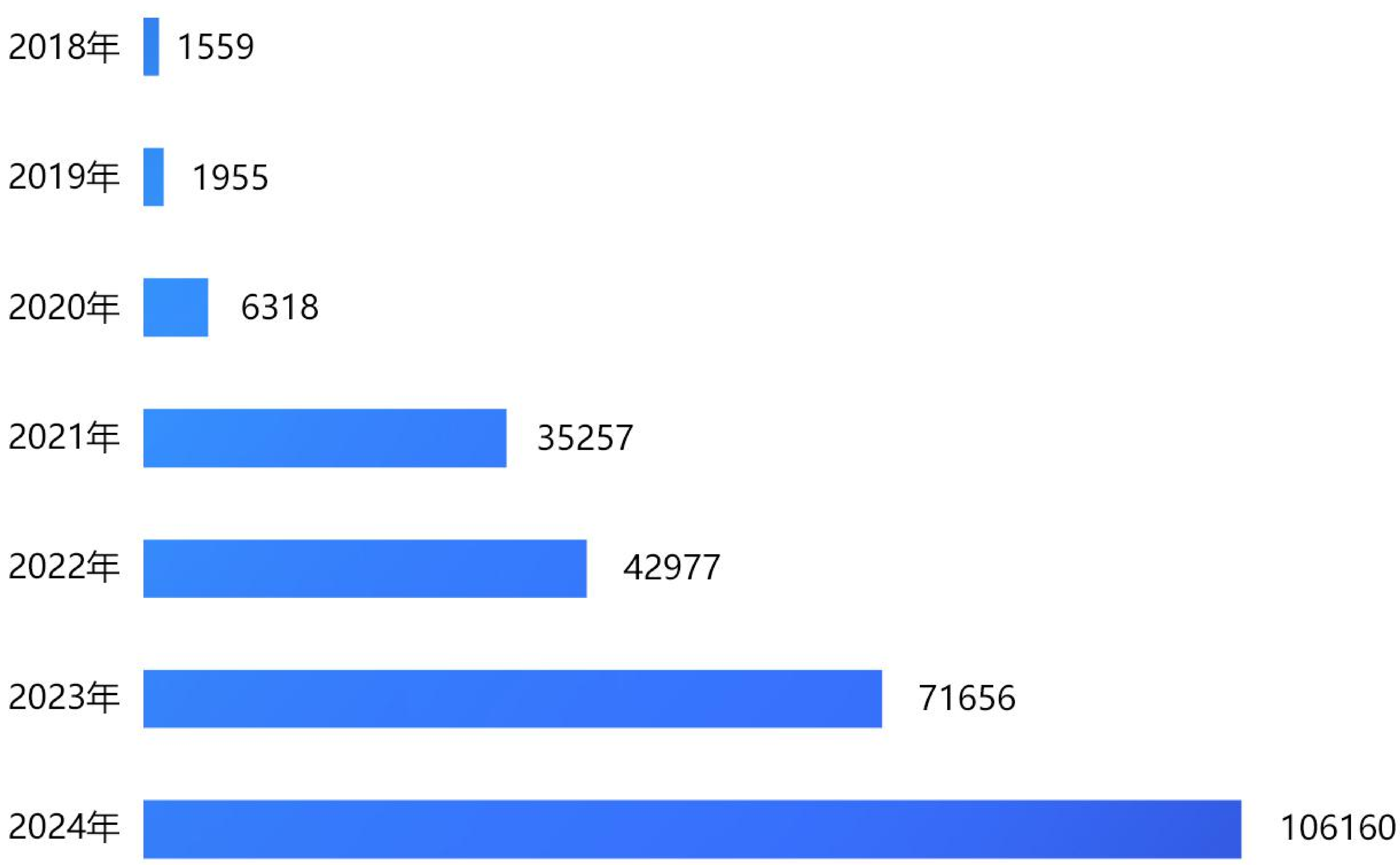
2024年，在PC游戏外挂样本中，射击类游戏依旧占比超过一半，从往年的55.43%增加到72.30%，其次为动作类、多人战术竞技类游戏。

2024年腾讯不同类型PC游戏监测到的外挂分布



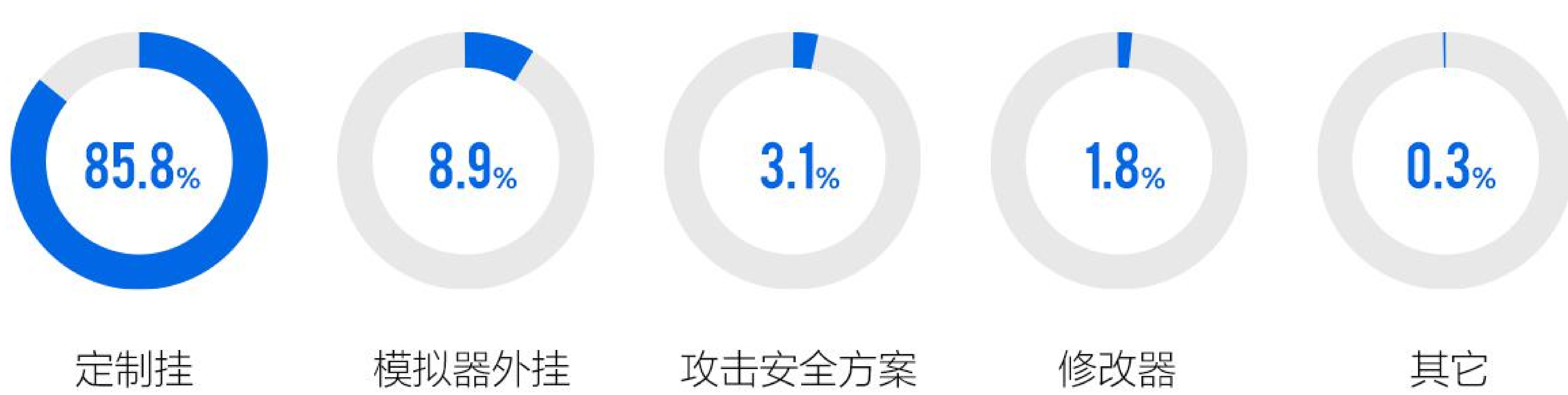
移动游戏外挂问题

腾讯移动游戏近年来对抗的外挂功能数



从腾讯游戏安全对抗的移动游戏外挂情况来看，2023年-2024年随着移动游戏市场出现增量，外挂功能数出现了明显增长。2024年移动游戏外挂功能数达到历史新高106160个，同比2023年的71656个增长48.15%，由此可见移动游戏外挂黑产问题依旧严峻，游戏厂商需要特别重视。

腾讯检测到的移动游戏外挂类型分布



2024年全年，腾讯游戏安全检测到的移动外挂中，定制外挂持续上涨占比达到85.8%，其次，模拟器外挂和攻击安全方案类的外挂分别占8.9%和3.1%，修改器占比为1.8%。相比通用修改器，定制外挂对抗难度更高。因为定制外挂具有更新频率快、实现式样变化多、集多个作弊功能于一体等特点，需要游戏厂商部署强有力的安全方案来应对。

外挂行业当前的特点

A PC端外挂价格持续上涨，普通内存挂价格从33元/款上涨至45元/款；由于DMA硬件外挂的黑产逐渐成熟，24年DMA硬件外挂的均价从23年的6000元下降至1500元，玩家作弊门槛持续降低。

B 据腾讯游戏安全检测数据显示，2024年大部分的外挂均为收费定制外挂、尤其是移动游戏，热门游戏收费外挂样本占85%以上。

C 受内核挂技术开源的影响，内核挂数量占比外挂大盘从16%增加到43%，均价从205元/款下调到146元/款。

外挂打击的难点

游戏作弊已经不是某一个地区特有的现象，当前，全球各地只要有热门游戏，尤其是竞技类游戏，就会催生出一条游戏外挂产业链，但是无论是对于PC游戏还是移动游戏，外挂的打击都充满挑战，原因如下：

外挂全球化

随着游戏的全球发行，同一款外挂支持全球多地区版本，尤其是非游戏发行商所在国的外挂样本获取难度增加

外挂AI化

随着AI技术与机器学习的不断发展，涌现出大量AI外挂。在不少知名的PC端FPS游戏中，均出现了AI外挂实现自动瞄准和击杀的功能，随着AI外挂对抗打击的深入，已出现AI+双机、AI+云机的作弊，让检测难度进一步增大

外挂硬件化

随着对抗不断深入，在PC游戏中，作弊者越来越多的使用同步器、双头盒子、鼠标宏、kmbox等硬件作弊方式去试图躲避检测。尤其是随着DMA技术的快速发展，通过硬件只读取游戏关键数据来实现透视等功能，给FPS游戏反外挂带来新的挑战

外挂隐匿化

外挂大量使用第三方有漏洞的驱动、内核Shellcode等高级隐藏技术，以实现作弊和躲避检测

外挂定制化

外挂一日多更，自动定时发布新版本；在作弊机器上，外挂可对自身文件，内存代码添加随机变化，使得一人一外挂样本，千人千面；在这种激烈的对抗形势下，传统的门槛级检测方案，或是一些短效的、点对点式的逻辑数据校验方案，已经不足以应对

外挂云更新

一个登录器对应多个外挂样本，登录器自动下载那些功能稳定且好用的外挂样本，实现云更新，即使单个外挂被对抗掉，玩家还可持续使用新的外挂

更高维度的作弊

使用外挂作弊已经不仅是停留在对游戏逻辑和数据的修改，也是与安全方案检测本身的对抗，比如PC游戏VT技术的使用

伪装性强

外挂利用网络流量限制，实现伪装成正常客户端的数据上报，绕过安全检测

抗测试

目前已有部分外挂，实现了对于外挂所在机器所谓安全外挂测试机的判断，并关闭外挂功能，从而在功能测试阶段即阻止安全侧的正常运营

外挂内核化

在计算机系统中，操作系统被分为用户空间和内核空间两部分。用户空间是运行普通程序的地方，而内核空间是运行操作系统代码的地方，它具有对硬件的完全控制权和对所有内存的访问权。当前，移动游戏的外挂已经出现内核化趋势，市面上已经出现内核挂，意味着它、更难以被检测和防御

另外，对于移动端游戏而言，黑产更是充分利用移动端系统下游戏权限较低的特点，利用外挂本身处于ROOT，越狱环境下的权限优势，进行跨进程的外部作弊。

02. 游戏经济安全问题

游戏内经济系统是指游戏通过虚拟货币、道具、资源和交易功能构建的经济生态。它既是游戏玩法的重要组成部分，也是维持玩家长期参与和厂商收益的核心要素。它旨在维持游戏内的经济平衡，确保玩家通过正常游戏行为获得合理的回报，同时保持游戏的公平性和可持续性。

游戏经济安全问题的分类

经济安全黑产围绕游戏内经济系统，通过寻找设计漏洞、高效获取资源、线下售卖获利、提供定制服务等方式来盈利。游戏经济黑产问题，可划分为三类

传统经济黑产

01

是指黑产团伙通过大量账号和第三方工具，获取、转移、售卖游戏资源所引发的问题，包括游戏资源超发，破坏游戏经济系统等。

渠道黑产

02

是指通过构建虚假账号、恶意自充值等行为，利用游戏渠道买量/分成规则，进行牟利的黑产团伙，会增加渠道成本。

服务型黑产

03

是指为满足玩家特定需求，通过批量账号和设备提供相应服务所引发的问题，破坏游戏公平性，影响玩家游戏体验等。

对游戏的危害

- 收益侵占

游戏黑产售卖的虚拟产品价格比官方便宜，吸引力强，导致部分玩家会选择从黑产购买，从而给游戏造成损失。同时也会让正常付费玩家感到不公平。

- 破坏游戏生态

大量黑产账号从游戏中获取资源，这部分系统超发资源进入市场流通后，导致游戏内的虚拟资源贬值，甚至绑架整个游戏经济，严重干扰了游戏的经济生态平衡，缩短游戏生命周期。

- 玩家体验

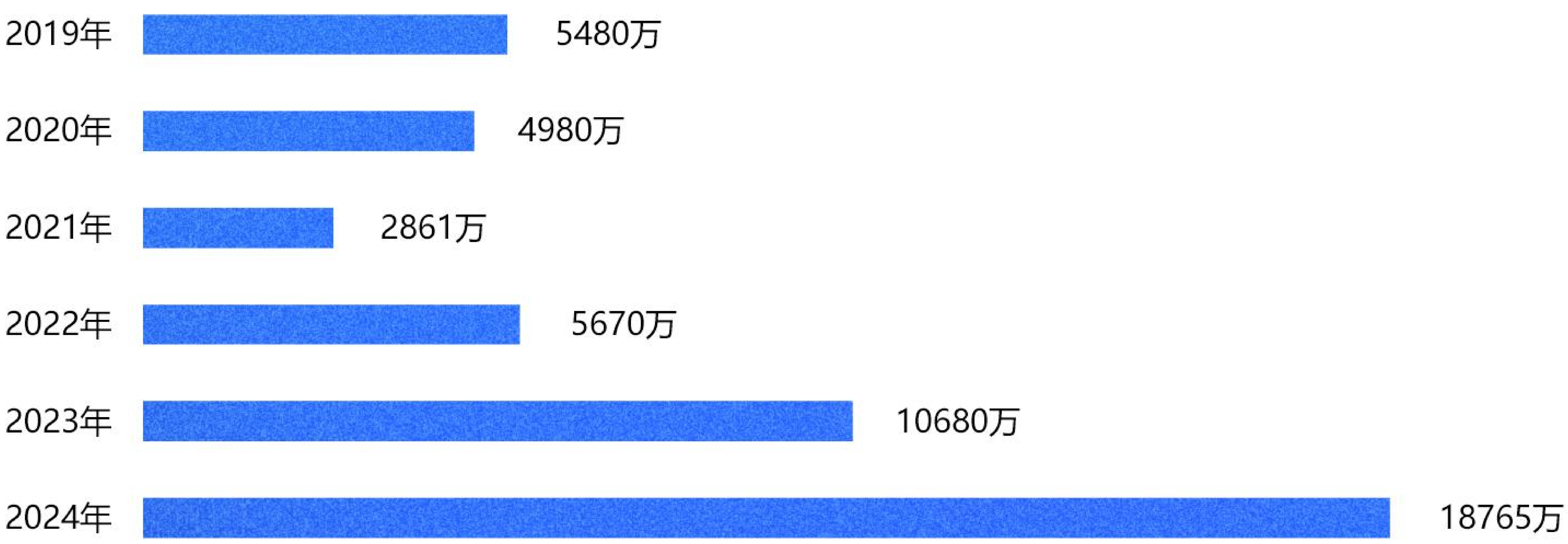
大量的黑产账号会挤压正常玩家的游戏空间（如新区进不去、抢不到怪、满屏都是挂机号），同时黑产的显性特征也会给玩家造成不好的游戏体验。

- 口碑影响

黑产对玩家体验造成的负面影响会使玩家对游戏不满，造成负面口碑传播甚至是社会上负面影响。

除此之外，在游戏开服期，黑产的恶意发言会影响前期玩家的留存。游戏运营中后稳定期用户形成对黑产的依赖后，就会影响游戏口碑，同时若单服收入较低，还会遭遇黑产的集体撤离，影响游戏长线运营的生命周期。

游戏经济安全处罚数据大盘



随着头部游戏上新增服务型黑产的检测与精细化管控和游戏新增玩法，从2023年起，黑产账号处罚总量出现了较大的增长。到2024年，全年处罚量18765万，相比2023年全年处罚量10680万增长了75.7%，2024年经济安全处罚数据变动的主要原因在于：

- 头部游戏对各类黑产（传统批量黑产、服务型黑产等）的打击力度都有不同程度的加强；
- 棋牌业务黑产入驻比较多，打击力同样显著加大；
- 国内海外游戏上线，对应黑产规模增长明显。

经济安全管控难点

随着黑产团伙越发成熟，管控难度也随之增加，需要持续迭代系统全面的技术和管控方案，来进一步限制黑产的规模和收益。总体来看，当前阶段难点主要表现在：

账号成本低

各大社交平台账号注册门槛低，大量黑产号涌入游戏作恶。账号源头管控难。

生产工具完备

云手机、虚拟机、同步器、模拟器、云代理IP、硬件修改器和自动脚本成为黑产的标配。

盈利模式多样

从传统资源售卖扩散到首充号、榜单人气黑产、陪练、活动营销等定制化服务。

影响更多维

黑产不仅影响游戏收入，还影响游戏口碑、服务器资源、玩家感知等等，单从封号无法根治，需要更定制化的场景治理。

产业链根深蒂固

黑产团伙已经形成了完整的产业链，从工具生产到最终变现分工明确，打击难度大。

交易平台便利性

交易平台的便利性极大提高了黑产变现的效率，同时也提高了打击对抗的时效性要求。

03. 内容安全问题

在游戏中，违规信息主要包括引流广告、辱骂、低俗等内容，其中具有游戏特色的引流广告，主要包括代练、代充、买卖金币、买卖外挂等。腾讯游戏内容安全检测系统覆盖的检测范围，涵盖了游戏及社区所有的用户信息发布场景，涉及文本、图片、视频、语音等信息载体。

违规文本检测大盘

2024年，腾讯游戏安全检国内渠道测到的一些主要恶意违规信息量级如下：

380.1亿条	44亿条	6979万条	223万条
辱骂信息	广告信息	游戏拉人信息	其他令人不适的信息

内容风控面临的挑战

1.量级庞大

每年，游戏黑产生产违规信息的量级十分庞大，数以亿计。并且形式也很多样，其中包括但不限于文字、图片、语音等。

2.复杂多样

除了游戏玩法内容本身，其他的违规信息一般是经由玩家发出的内容，通常的违规内容包括辱骂、广告、色情等不健康内容，及其他违法和不良信息。

3.迭代多变

为了躲避系统检测，违规信息也一直在更新迭代。违规用户尝试用谐音字、象形字、文字加拼音、上下文的方式绕过检测。同时因为一些新闻时事，会出现某些特定“地域黑”敏感词汇，影响玩家体验。

不同游戏类型面临的主要内容风控问题

不同游戏类型的面临的违规内容类型也不尽相同：

- 所有游戏类型如缺乏管控，均容易出现低俗及其他违法不良信息；
- MOBA 游戏更容易出现辱骂类违规信息；
- 射击类游戏更容易出现外挂广告和辱骂类违规信息。

由于形式多样，所以违规信息涉及到的场景也非常多

文本类违规信息主要出现在：

昵称　聊天窗口　邮件　弹幕　房间名　邮件里　名片签名里

- 图片类违规内容主要出现在:

头像　相册　动态　空间　群聊　社区内

值得注意的是，除了常规的辱骂、广告和低俗违规信息，有一类在游戏中比较特殊的现象，就是游戏的拉人问题。近年来，腾讯游戏安全发现在不少的游戏中，黑产团伙会在游戏中发表收徒、组车队、送皮肤等各式各样的言论或语音，吸引玩家加好友后，给玩家发送联系方式进行引流。有的甚至不在"世界频道"活跃，通过添加玩家为好友或直接私聊已有好友进行引流，玩家甄别能力弱，遭到诈骗的风险极高，给玩家的游戏体验造成巨大影响。

04. 账号安全问题

盗号产业发展的成因

- 经济利益驱动

游戏内物品如稀有皮肤、虚拟货币等具有较高的经济价值，盗号者可以通过出售这些物品获取非法收益，还有的游戏账号绑定了个人信息和支付方式，盗取后可能获得非法收益。

- 市场需求存在

部分玩家对低价游戏账号和虚拟物品的需求，或者想作弊但又怕使用自己常用的游戏账号会被游戏公司封禁，就主动找途径购买账号，这些都为盗号产业提供了市场空间，形成了从盗号、洗号到销售的完整产业链。

- 技术手段成熟

黑客技术的发展使得盗号手段更加多样化和高效，如恶意软件、钓鱼网站、撞库等手段的广泛应用。

- 监管难度大

网络环境的复杂性和盗号行为的非强聚集性，使得监管和打击盗号的难度较大，作恶成本相对较低。

盗号方式多样，对抗挑战大

当前盗号方式有恶意软件、钓鱼诈骗、撞库攻击、租号借号、社交工程诈骗等，每一种方式都十分隐蔽，对抗挑战大。

恶意软件

包括病毒和木马，黑客利用病毒或木马程序窃取玩家的登录信息。这些恶意软件通常通过伪装成第三方工具、外挂或破解程序分发。在所有的盗号方式中，木马盗号产生的影响更大，在某些地区，公共网吧中可能存在用于窃取账号信息的木马程序，尤其是缺乏安全管理的场所。

钓鱼诈骗

不法分子搭建与游戏官方高度相似的钓鱼登录入口或链接，骗取玩家登录凭据和个人信息。

撞库

黑客利用从其他数据泄露中获取的用户信息，尝试在游戏账号登录界面通过自动化工具进行批量登录。部分玩家在多个平台使用相同密码，容易被撞库成功。

租号借号

玩家通过租赁服务短期使用高等级账号，也有部分地区因私下借号行为导致账号信息泄露。

社会工程学诈骗

黑客通过伪装成客服、官方人员或可信任的第三方，诱导玩家泄露账号和密码信息。

账号共享

玩家把账号共享出去后，其中一个人的设备被黑或者密码泄露，攻击者就能轻松获取账号。另外，共享时可能通过不安全的渠道传递密码，比如短信、社交媒体，这些都可能被拦截。

盗号的影响

■ 对玩家的影响

玩家账号被盗后，可能由于恶意行为造成账号的封禁，或者存在账号资产转移、毁号等，对号主产生影响。

■ 对游戏的影响

盗号是很多游戏安全问题的源头，黑产盗号后自己或卖给其他黑产用于外挂作弊、恶意发言、经济黑产等系列恶意行为，对整体游戏安全造成影响，同时影响原号主游戏可能产生弃游，对游戏的活跃、收入都产生间接影响。

■ 对行业影响

被盗账号常关联手机号、身份证等敏感信息，黑客可能通过撞库攻击进一步窃取其他平台账户，或利用隐私数据实施精准诈骗，盗号者甚至通过社交关系链实施二次诈骗，造成连锁伤害。

解决盗号问题的困难和挑战

■ 技术对抗复杂

黑客技术不断进化，安全防护系统需要持续升级以抵御新型攻击手段。

■ 玩家安全意识薄弱

许多玩家缺乏基本的安全意识，例如设置弱密码或轻信钓鱼信息，增加了账号被盗的风险。

■ 攻击手段的多样化

黑客可能同时利用技术手段和心理诱骗，增加了防范的复杂性。

■ 多平台防护难度大

有的玩家的游戏账号可能在多个平台使用，每个平台的安全防护措施不同。

■ 打击黑色产业链的执法难度

盗号团伙匿名性强，取证和执法过程复杂且周期较长。

05. 营销推广作弊问题

营销推广作弊，在游戏领域通常指厂商在游戏内外进行营销推广时，黑产通过技术和人工手段操纵结果，伪造正常或者优秀的营销效果来获取厂商的营销投入，甚至还可能误导厂商对营销推广做出错误判断，造成直接经济和市场损失。

游戏领域常见营销推广作弊方式

低价营销

分成模式下，利用低价营销策略吸引用户，形成对其他渠道方的恶性竞争，进一步影响产品用户在不同渠道下的付费公平性，如作弊渠道以首充号折扣来吸引用户

假流量（点击、播放、人气等）

作弊方通过人为程序或操作，模拟需求方真实流量，或者上报虚假数据，但实际上没有真实用户参与

低/劣流量

A 各类变体的积分墙形式，作弊方通过实物或现金吸引羊毛党完成需求方产品的下载、注册、对局、分享等特定行为，用户完成任务领奖即走，直接影响需求方产品留存与付费数据

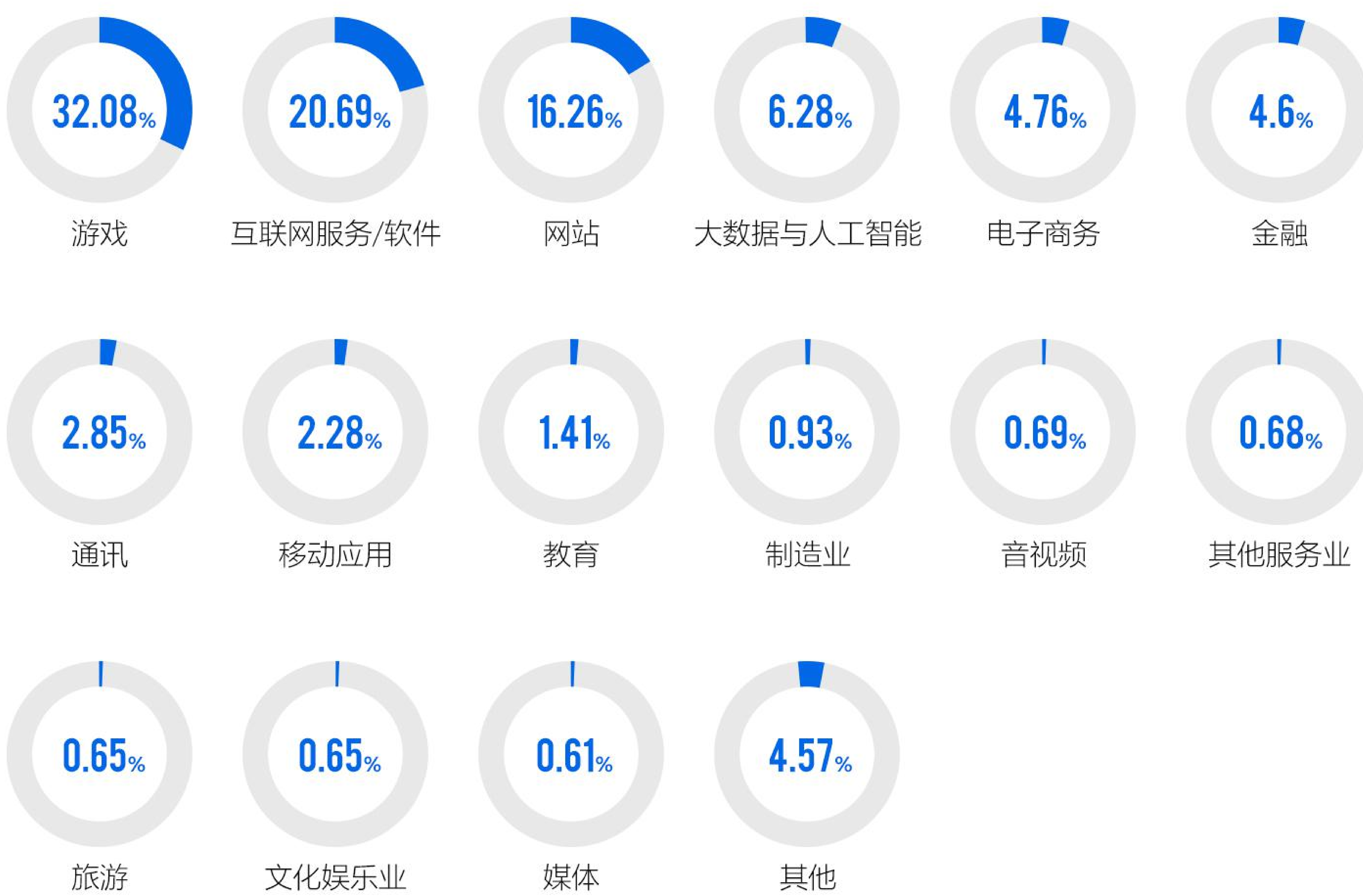
B 各类变体的撞库操作手法，作弊方结合流量池内真实用户行为或者所掌握的真实用户画像，夸大或虚假上报需求方目标流量，撞库需求方新进/回流用户，攫取其他流量供给方收入，且影响需求方在流量选择上的战略决策

C 各种对自然流量的"注水稀释"类行为，通过上述人为模拟或积分墙等操作方式，将真实流量中混入虚假与低劣流量，刻意控制质量在需求方可接受程度，使需求方单位真实用户付出更高成本

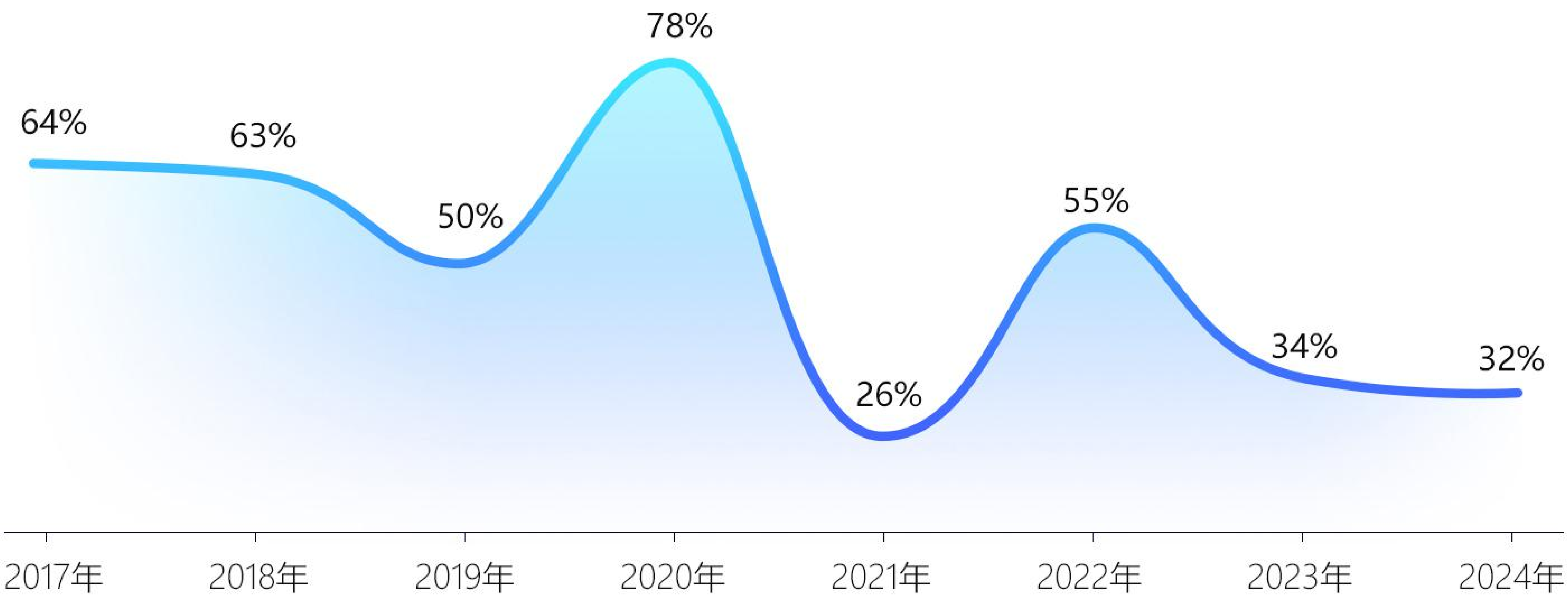
06. DDoS攻击问题

游戏行业DDoS攻击为全行业最高

互联网技术的多元化生态和高速迭代进程，使得数字经济发展迅猛的领域正面临愈发严峻的网络安全挑战。根据腾讯DDoS防护团队统计，2024年全球攻击数据显示，游戏、互联网服务/软件、网站服务、人工智能及大数据四大领域已成为DDoS攻击的重灾区。其中，**游戏行业的DDoS攻击在全行业的占比达到32%，占据所有行业的最高比例，游戏厂商遭受DDoS攻击几乎已经成为常态。**



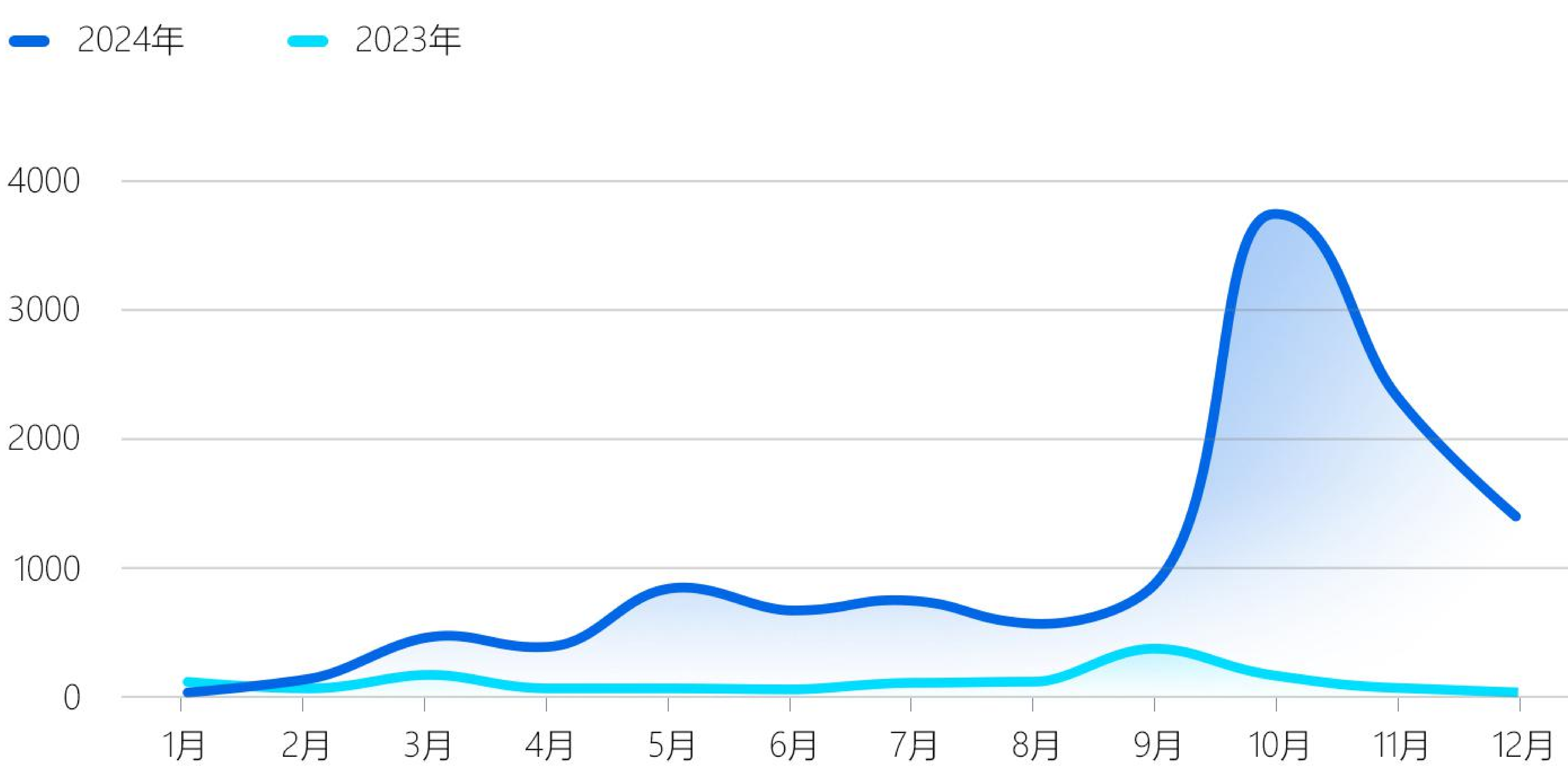
■ 游戏行业DDoS攻击在全行业占比



游戏出海DDoS攻击威胁加剧

近年来，随着国内游戏市场竞争日益激烈，游戏发行商纷纷将目光瞄准了空间更为广阔的海外市场，游戏出海俨然已经成为了中国文化内容出海的主力军。而游戏行业作为DDoS攻击的重灾区，伴随市场红利而来的安全威胁呈现指数级技术对抗态势。同比2023年，2024年针对海外游戏的DDoS攻击次数和攻击流量峰值均有明显上涨，攻击次数上涨893%（24年10月同比23年10月攻击次数上涨量达到26倍），对游戏业务的正常运营造成严重威胁。

■ 2023-2024年出海游戏被DDOS攻击的次数

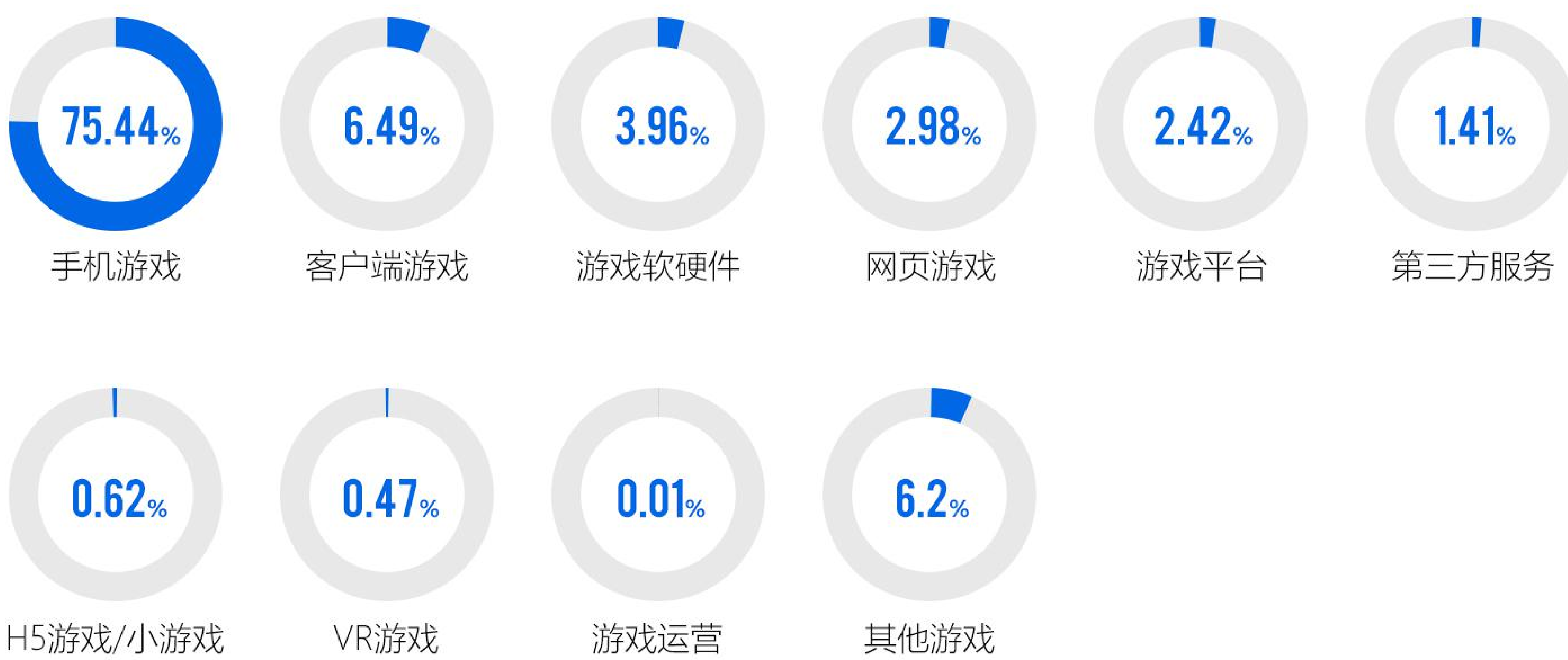


■ 移动游戏成为DDOS攻击最主要的游戏品类

手游依然是DDOS攻击最多的细分游戏品类，23年手游在游戏行业整体DDOS攻击中的占比就超过游戏行业的三分之二的攻击比例，24年呈持续扩大的趋势，占比进一步接近8成。

端游的攻击占比从10%下滑到6.49%，但是仍然是攻击第二多的细分品类，在游戏行业攻击占比接近1成

页游作为去年占比第三高的细分品类，今年的占比较去年则有较大幅度的下滑（近7成）



DDoS攻击团伙获利模式

攻击团伙敲诈勒索、游戏玩家恶意作弊或者报复、行业内恶意竞争仍然是DDoS 攻击最主要的攻击动机，这在游戏行业内尤为典型。

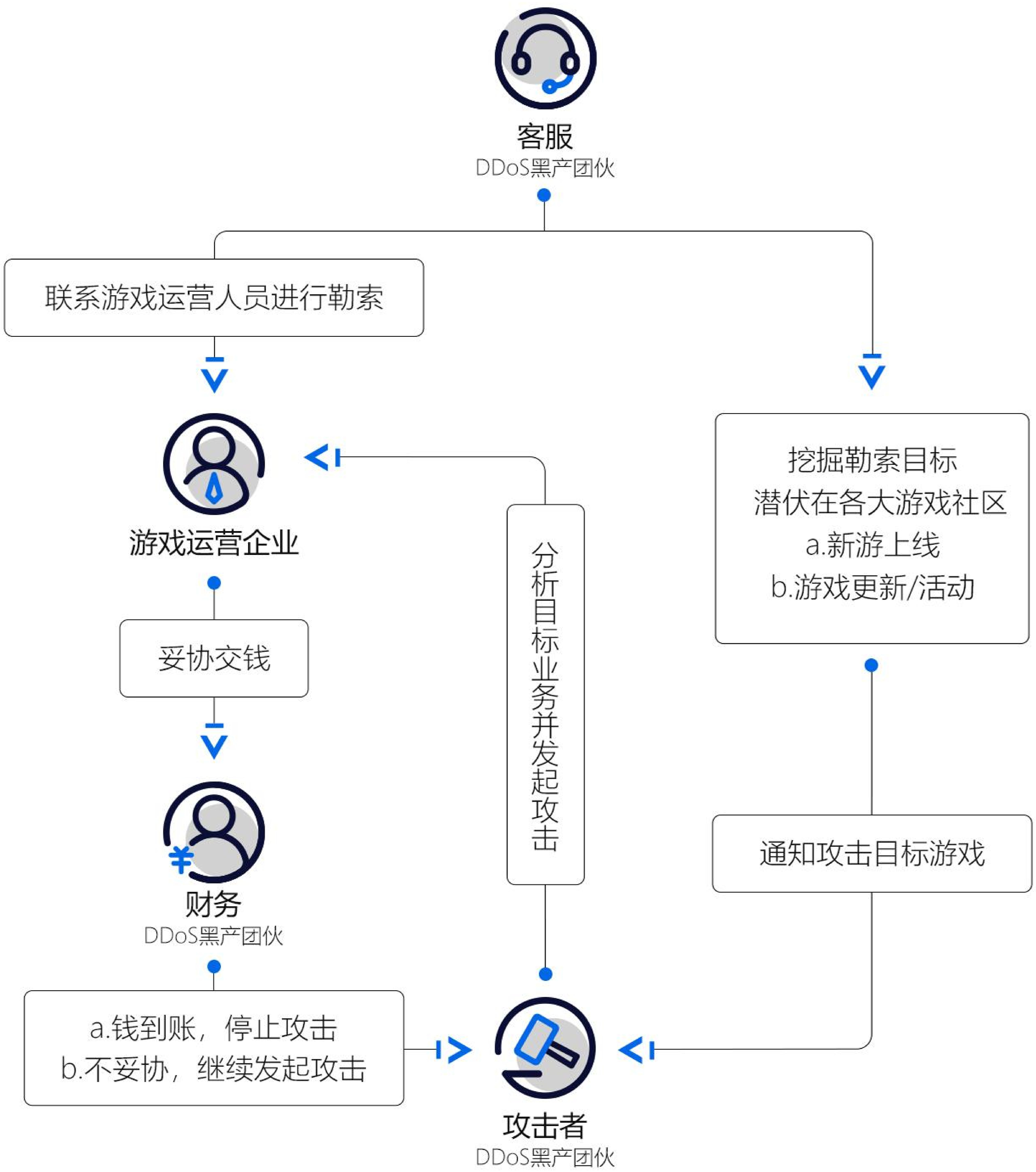
■ 攻击团伙敲诈勒索

企业一旦遭到攻击，为确保游戏稳定运营不得不快速做出让步，致使敲诈勒索的成功率相对更高。

AI技术的突破，也全面升级了黑产们的工具生态，大幅降低黑产门槛，如某DDoS勒索组织借助大模型生成其DDoS攻击脚本，可自动化生成攻击指令。而且，黑产团伙会特意针对游戏上线当天进行DDoS攻击勒索，索要大量“保护费”。以某著名DDoS攻击团伙为例，其获利的主要模式是对游戏行业在新游上线/版本更新/游戏登榜之后发起敲诈勒索为主要获利方式，具体的勒索金额会依据企业规模大小以及收入情况会有所不同：

1.对于中小开发商，勒索金额在1万元至2万元之间，以公司维度收费；

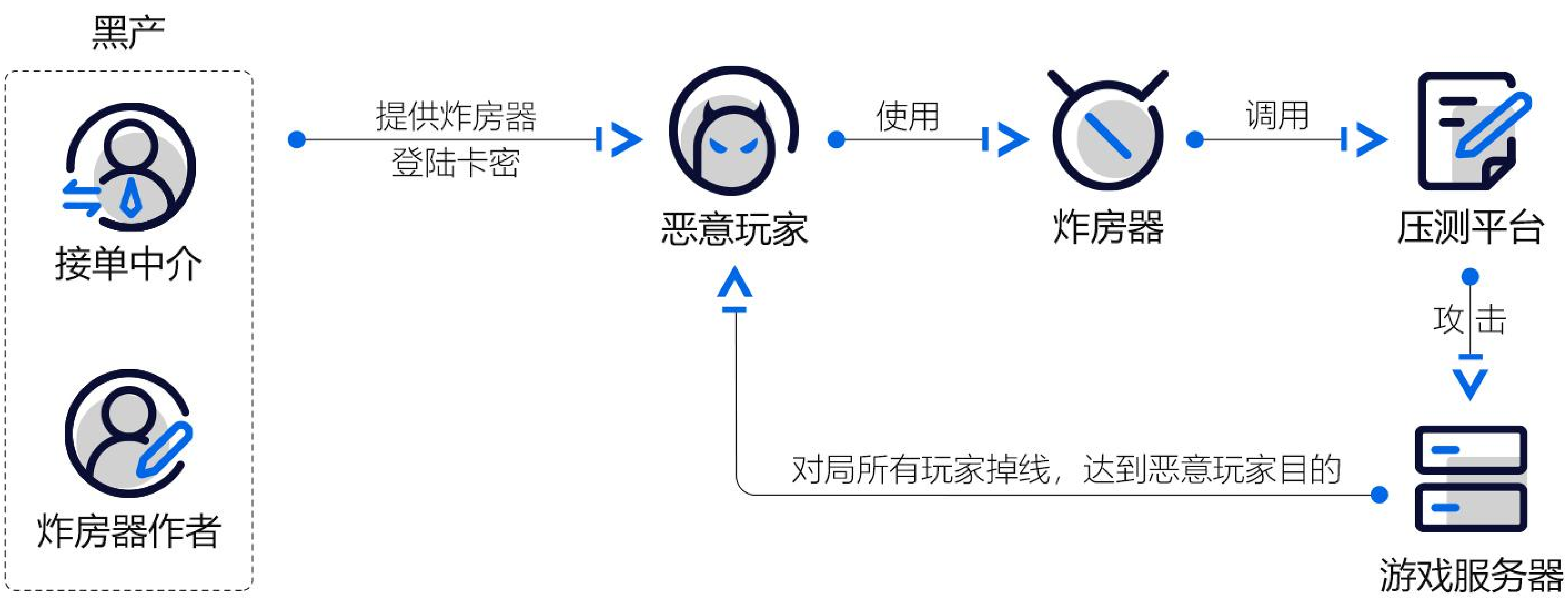
2.对于一些业界有一定知名度或收入较高的游戏厂商，勒索金额会提升到数万元至数十万元，收费维度也会细化到单个区域或者单款游戏；



游戏玩家恶意作弊或报复行为

一方面，恶意玩家为获得游戏内非公平性收益，发起DDoS炸房（对局作废稳定上分、快速提升段位、快速收割拿人头、代练工作室等），另一方面，部分玩家因装备丢失或封号，购买DDoS服务宣泄不满，形成灰色产业链。

典型的DDoS炸房黑产链条



07. 其他游戏安全问题

除了上述常见的安全问题以外，游戏中还常常面临着其他的安全问题，包括消极游戏、演员、代练、"带老板"、"观战透视"等，其中消极游戏又包括挂机、送人头、恶意组队、故意伤害队友等。

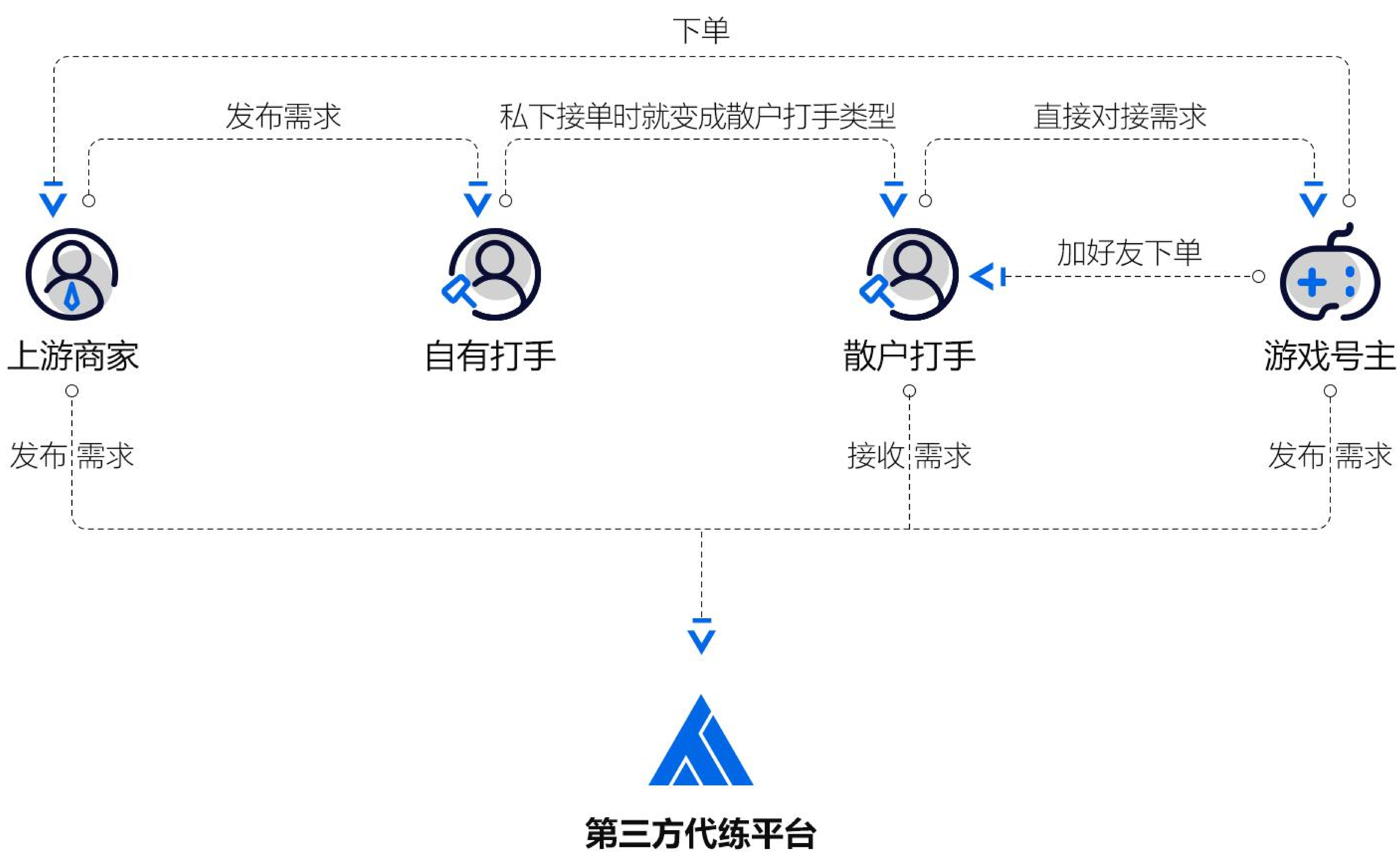
代练

游戏代练通常由技术娴熟的游戏玩家或者公司提供，他们会代替普通玩家玩游戏，以提高玩家账号在游戏中的等级，获取特定的物品、技能或荣誉等，普通玩家通常需要为这种服务付费。

代练会破坏游戏环境，在一些竞技游戏中，代练可能让一些玩家的技能水平看似超越了他们实际的水平。这不但对那些真正提升自己技能的玩家不公平，也可能在玩家间产生混乱，比如在队伍协作的游戏中。同时，代练还会对游戏的经济系统产生影响，尤其是在那些允许玩家之间进行物品交易的游戏中，大量的代练可能会导致游戏货币的通货膨胀，使得物品价格上涨，影响正常玩家的游戏体验。

代练还会涉及到游戏的账号安全问题，一些代练团伙可能会在获得账户访问权限后窃取玩家账号或者其中的虚拟财产，或者利用账户进行违规行为，这可能会导致原账户所有者的游戏账户被封禁。

当前游戏代练产业发展成熟，网络上各种的代练中介平台和被利益驱动的代练打手越来越多，号主、上游商家、打手、代练平台之间已经形成了一条完整的黑产产业链。



演员

“演员”行为，一般指的在游戏中，存在“送分”和“吃分”的玩家，在同一对局中，操纵比赛结果的恶意行为，一般出现在MOBA游戏对局中，有时也会出现在FPS游戏中。

“演员”基本分布在高段位排位对局，是有组织有计划地人为操纵比赛结果从而达到特定目的的行为，送分和吃分玩家存在利益关系，这是区别于普通的消极游戏行为的一个最大的特点。

近年来，随着腾讯游戏安全演员检测技术的日益提升，MOBA游戏的演员行为不再像过去一样明目张胆，而是日趋隐蔽。除了传统的吃分送分行为外，还出现了专门针对头部游戏主播或者职业玩家，操纵比赛结果，进而参与博彩外围获利的演员行为。

- MOBA博彩演员行为特点

博彩网站

引流

游戏内广告

游戏、直播露出引流
影响1000万人次/天

下注

游戏内广告

假赛操纵游戏胜负狙
击百万粉丝KOL

狙击

雇佣

开盘

开盘直播、赛事

博彩庄家

- 匹配到主播对局，多个演员操纵对局
- 演员通常采用多赛季正常活跃账号，账号过去无类似的违规行为

挂机、送人头

■ **挂机**：这通常指的是玩家在游戏进行时，自己并没有操作角色，而是让角色静止不动或者使用自动战斗功能。挂机行为可能是因为玩家离开了电脑或游戏设备，或者是为了利用游戏的机制来获取经验或资源。

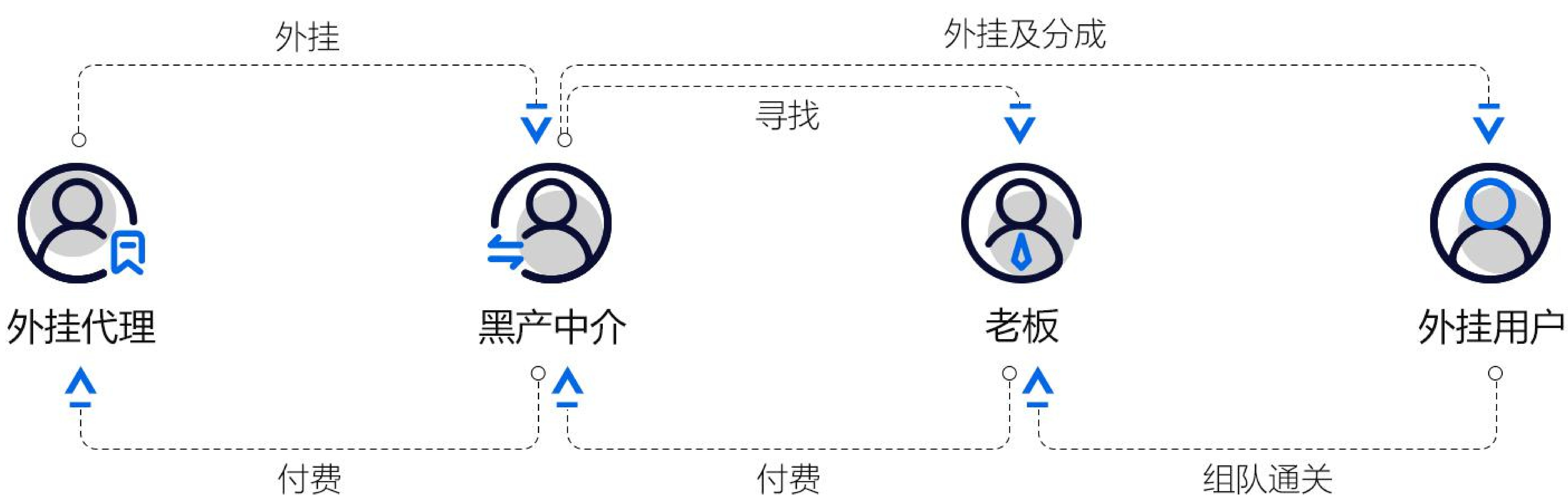
■ **送人头**：指的是玩家故意或者因为操作失误导致自己的游戏角色被对方玩家击杀，也就是给对方送去了一次击杀（被称为"人头"）的机会。

挂机行为对游戏和其他玩家都有一定的影响，比如，在需要团队合作的游戏中，挂机玩家可能会导致团队人数的失衡，使得其他玩家面临更大的挑战。此外，挂机也可能影响到游戏的经济系统，因为挂机玩家可能会获取到大量的资源或经验，从而破坏游戏的平衡。

送人头会直接影响到游戏的结果。在MOBA类游戏中，每次击杀都会给击杀者带来经验和金钱，因此送人头会使对方玩家变得更强，从而影响到团队的战斗力。此外，送人头也可能会影响到其他玩家的游戏体验，因为这可能会导致游戏的失衡，使得他们在游戏中面临更大的困难。

“带老板”现象

“带老板”是指玩家（老板）加入到开挂的队伍中，与开挂玩家组成一队，在游戏中快速获益。在不同的游戏中，“带老板”又有不同的叫法，有的叫“坐挂车”，有的叫“坐飞机”。目前“带老板”已经有成熟的商业模式，外挂代理、黑产中介、外挂用户有着明确的分工。



“观战透视”现象

“观战透视”主要存在射击竞技类游戏中，指的是玩家在游戏小号中使用透视外挂来观战大号的方式进行作弊，通常存在于FPS游戏中。

“护航”作弊现象

“护航”作弊主要存在于射击竞技类游戏中，“护航”的玩家分为两队：一队是上交了保护费的“老板”玩家（主要目的是上分）、另外一队用高段位大号（“司机”）组队带上一个开挂的小号（“打手”）。两队同一时间开启匹配，提高匹配到同一局的概率。“司机”成功将“打手”送入高分段对局后便退出游戏，而后“打手”负责淘汰其他玩家，“老板”则等待到最后决赛圈击败“打手”，直接成为冠军。

08. 海外游戏安全问题

伴随着越来越多游戏厂商的出海，海外的游戏安全问题同样值得关注。相比国内，在海外由于存在不同国家和地区的文化法律差异以及玩家游戏习惯的不同，其游戏安全问题也会有所不同。

海外游戏安全问题一览图

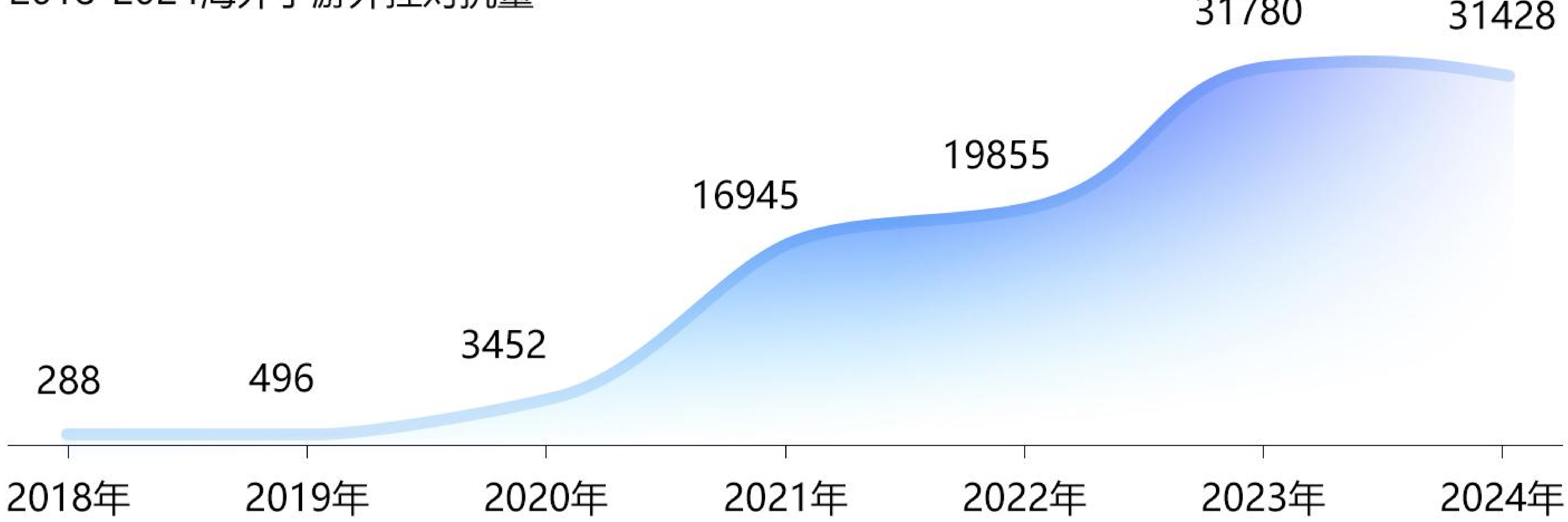
外挂作弊	经济类黑产	更多不良行为	账号安全	多语种内容安全
修改数据	**刷初始号**	演员、默契比赛作弊、恶意组队	**平台账号被盗**	**不同地区和国家的文化禁忌**
修改代码	机器自动化打金	消极游戏行为	**邮箱被盗**	辱骂内容
修改协议	控制道具流通售卖游戏资源	干扰、蓄意战败	**账号恶意绑定**	诈骗类内容
破解游戏客户端	**代充等**	代练等	财产损失	引流和广告类
辅助插件等				

海外的游戏安全问题既有跟国内相似的、游戏经济类黑产问题、账号安全问题和其他违规行为，同时也因为不同地区和国家的文化差异，存在着更为复杂的内容安全问题。游戏厂商在出海前，应在一定程度上提前部署游戏安全一揽子方案（包括技术、法律、政策等多方面）。

海外游戏安全问题一览图

- 海外手游外挂量变化

2018-2024海外手游外挂对抗量



根据腾讯游戏安全的数据统计显示，ACE在2024年对抗的海外手游外挂量为31428款，与2023年全年的数量基本接近，作弊功能类型超300种，海外的外挂主要通过电报传播。

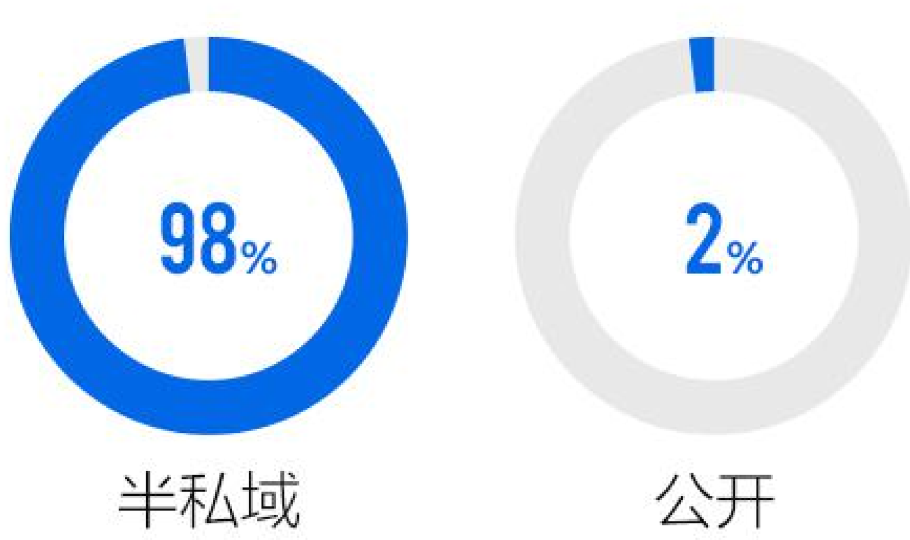
另外，因海外的游戏账号注册成本更低，因此，海外的外挂作弊更倾向于显性作弊。很多玩家即便因开挂被处罚后，仍继续换号进行作弊，因此海外的安全对抗对于作弊检测的时效和覆盖的全面性有更高要求。

海外外挂类型分布及溯源

2024年腾讯海外移动游戏检测到的外挂类型分布

跟国内的外挂类似，在海外，定制外挂占大多数，其次为模拟器外挂和修改器，需要游戏厂商的反外挂技术不断深化。

海外手游外挂传播渠道



由于在海外的外挂产业链中，外挂黑产转移成小群体，98%的外挂是通过通过私域/半私域（如电报）交换信息，仅有极少部分的外挂是通过公开渠道（如网站、论坛、社媒等）传播，因此获取外挂样本的难度更高。海外反外挂工作也涉及不同国家和地区的法律、社会制度，开展反外挂工作时所面对的情况也非常复杂。

不同地区的文化差异对内容安全方案要求更高

海外的内容安全问题中，除了常见的色情、暴力、辱骂、低俗、广告引流等信息，还因为不同地区的文化差异，有不同的文化禁忌。

了解和遵守各地的法律要求和文化禁忌是确保游戏在全球范围内成功的关键因素之一，不同的国家地区在法律法规、政策以及文化、宗教信仰上有不同的要求，尤其是，目前许多国家已推出相关法律法规，要求平台方设置内容审核机制和规则保障内容合规，如果违规内容不能及时有效处理，则可能发生合规风险。与此同时，海外地区语言众多，要求内容安全方案具备强大的语言适配能力，精准识别相关的违规内容及变体内容。

1.通用的内容安全问题

海外地区，在游戏的UGC场景中，存在着各种色情、暴力、辱骂、低俗、广告引流信息，要求游戏厂商精准识别。

2.文化禁忌问题

每个地区都有自己特殊的禁忌，如一些地方禁止描绘某些动物或特定人物（例如皇室成员），或者某些颜色和数字可能带有不吉利的含义。这对内容过滤规则的设定提出了更高的要求，一不小心就可能引发公众的不满和抗议，甚至会造成法律合规问题。

3.宗教信仰问题

不同地区的宗教有着不同的文化差异，对游戏UGC内容的筛选和呈现方式提出更高的要求。

4.社会价值观差异

比如对性别平等、性取向、种族平等等社会议题的处理，不同地区可能存在极大的观念差异。

5.用户数据隐私保护问题

不同地区的文化和法律环境对于信息隐私的理解和保护程度有所不同，因此，游戏厂商在全球范围内部署内容安全方案时，必须充分考虑到这一点。要求厂商在数据收集、存储和处理等环节都必须严格遵守当地的法律法规，并尊重用户的隐私权。

总的来说，不同地区的文化差异要求我们在制定和执行内容安全方案时必须谨慎、周全，尊重当地的文化、宗教、法律法规和政策。

腾讯游戏安全针对出海游戏在接入安全服务过程中会遇到的合规问题，规范了在数据收集、保存、处理、回传、审核等环节各方的相关行为，确定了业务必须具备的安全能力基线，旨在遏制个人信息非法收集、使用等乱象，最大程度地提高业务在海外运营过程中的安全合规能力，为业务顺利出海保驾护航。

各类游戏安全风险的应对指南

THREAT MITIGATION STRATEGIES

03.

各类型的游戏都面对着各自独特的安全挑战，这些挑战来自于广阔的网络世界，犹如无形的病毒，潜伏在每一个角落，等待着游戏厂商的一次疏忽大意。然而，这并非是完全无法预防的，更不是全部都无法避免。游戏厂商应该提前预见这些风险，采取必要的措施，全面提升游戏的安全性。

在游戏的开发和上线阶段，游戏厂商应当已经开始关注并解决这些安全问题。这可以通过自建游戏安全团队，或者选择接入具有专业能力的第三方游戏安全服务来实现。这两种方式都可以在一定程度上遏制各类安全问题的发生，让玩家在享受游戏乐趣的同时，也能享受到安全的游戏环境。

作为广东省游戏产业协会游戏安全专委会的主任委员单位，腾讯游戏安全一直以来都积极联动行业同业者积极探讨，在应对各类游戏安全问题上也一套较为完善的方案。自2019年起，腾讯游戏安全便开始发布年度游戏安全报告，并于2021年起升级为《游戏安全白皮书》。我们在此针对游戏的各类问题，分享应对方式，以期在日常面对各类安全问题时，游戏厂商能够有所参考，做出最有效的处置。

01. 游戏外挂问题的应对

面对复杂的外挂问题，游戏厂商可以从事前、事中、事后3个阶段来开展针对性的措施。

事前

以防范为主，开展安全评审、加密数据、准备各类处置手段等工作。

安全评审

在游戏上线前，对游戏的安全性进行评估，对游戏版本进行漏洞挖掘及风险评估，并对潜在的漏洞和风险进行修复，并准备应急预案。

客户端加密和反外挂方案接入

对客户端的代码、组件、资源等进行加密和保护，防止客户端代码、资源被破解、调试等，提升客户端自身的安全性，可以寻求第三方反外挂方案，提前接入。

准备处置手段

为了在运营过程中，及时对作弊玩家和外挂进行处置，在运营前我们需要提前拟定详细的用户协议和游戏规则。

事中

以检测和对抗运营为主

建立安全运营体系

包含作弊监控体系、实时检测体系、作弊处罚体系以及客观衡量游戏安全性的指标体系。

舆情监测

对游戏外挂信息进行摸排，舆情信息及时测试和确认，情况属实的加入对抗流程。

搭建处罚体系

游戏运营方可通过搭建闭环处罚体系更精准地处置外挂用户。通过官方渠道定期发布反外挂措施和打击效果，提升用户对安全建设的参与和感知。

建立证据库

在合法合规的情况下，注意建立作弊账号违规的证据库。同时积极追踪外挂软件的来源，并获取部分有价值线索。包括：外挂制售方信息、外挂传播路径和交易信息等证据。确保证据的完整性和安全性，以备后续跟进法律途径使用。

事后

以用户运营及法律追诉为主

用户运营

为不同类型的用户提供对应的运营手段，进一步巩固反外挂运营的效果。

- A 对于作弊用户，提供处罚查询及申诉的功能，同时利用安全活动，引导玩家绿色游戏。
- B 对于被作弊玩家影响的用户，提供举报反馈服务，让用户感知到作弊玩家已被处理。
- C 对于正常用户，主要利用正向激励手段（如虚拟物品奖励、特权奖励等），结合实名认证及安全宣传，引导用户养成良好的游戏习惯。

法律途径

- A 就违法违规行为提起相应民事诉讼，追究侵权、违约或其他民事责任。
- B 移交有关行政管理机关给予行政处罚。
- C 移交司法机关追究刑事责任。

腾讯游戏安全方案

目前，腾讯游戏安全在外挂问题的应对上，已经有着20年的经验沉淀，尤其是在客户端加固、反外挂方案、服务端安全方案、外挂样本监控、定制外挂的检测与对抗、作弊用户处罚等维度，无论对国内还是海外的游戏，已经形成强有力的方案体系，**现已向业界提供安全方案，欢迎联系免费试用。**

方案类型	简述	效果
客户端加固	游戏上线前进行加壳处理，代码加密，防止游戏破解版	提升作弊门槛，防止游戏出现破解版
通用外挂检测和对抗	行业领先的反外挂方案，主动检测修改器、变速器、虚拟机等通用外挂，一经发现，立即弹框/闪退。同时提供腾讯反外挂能力接口，自助定制对抗策略	有效对抗通用外挂
服务端安全方案	通过服务端策略与客户端方案联动，有效对抗供给安全方案类的外挂，使用双数据通道实现更可靠的检测数据，且结合18种服务端策略显著提升外挂覆盖率	有效对抗攻击客户端安全方案类的外挂
外挂样本监控	腾讯ACE团队通过多种专业渠道，收集游戏外挂样本，验证外挂功能	及时、全面的外挂收集，尽早对外挂进行分析和对抗
定制化外挂检测与对抗	腾讯ACE团队对外挂作弊功能和原理进行详细分析，制定策略，进行对抗，提供动态安全方案和后台策略对抗方案两种机制，检测涵盖近两年新型的DMA硬件挂和AI挂。	专业的外挂原理分析报告，及时的外挂对抗效果
漏洞挖掘	腾讯ACE安全专家对游戏进行分析，挖掘游戏漏洞，提供修复建议	提前发现游戏漏洞提前修复，提升游戏安全性，提升外挂作弊门槛
模拟器对抗	在帮助游戏对模拟器玩家进行识别，做匹配隔离的基础上，可以采用腾讯手游反外挂+腾讯端游反外挂综合方案，对模拟器外挂进行深层次对抗(需指定腾讯手助为唯一可用模拟器)	对模拟器外挂进行有效对抗/模拟器建议与支持
作弊用户处罚	腾讯ACE团队根据检测结果，对游戏内作弊用户发起处罚建议	处罚作弊用户/提供处罚建议，协助业务做精细化策略
处罚申诉审核	针对游戏反馈的申诉案例，ACE团队进行证据核对，并提供核查结果	针对玩家处罚投诉等问题，进行针对性排查，给出答复

方案支持：

安卓 **iOS** **windows** **国内游戏** **国内厂商出海游戏** **海外游戏**

02. 经济安全问题的应对

游戏打金工作室类账号对游戏经济系统的破坏巨大，需要游戏厂商接入一套强有力的经济安全方案来持续检测。目前，腾讯凭借着多年的经济黑产对抗，建立了一套全面的经济安全方案，游戏厂商可以从以下维度来评估和参考。**当前腾讯游戏安全已向业界提供游戏经济安全方案，欢迎联系免费试用。**

经济系统风险评估

结合游戏玩法，对游戏可能存在黑产风险玩法进行全方位评估，并给出相应的解决方案，从玩法层面上降低黑产风险。

黑产账号、黑产交易检测

从传统机器学习升级为深度学习，更精准的检测黑账号&黑交易，让游戏侧在对玩家账号、黑产交易进行处置时，有更充分的依据。

渠道黑产稽核

对渠道假量、黑产充值行为进行稽核和管控，降低对渠道发行过程中的成本损失。

线下黑产规模大盘

将黑产规模映射到现实货币进行数字量化，让游戏侧可以从宏观层面把握游戏黑产的规模，同时进行管控之后，也能很直观地看到经济挽回的效果。

定制管控方案

传统的封号打击升级为管控手段，深入结合游戏特点和需求，更全面保障游戏经济系统健康，降低黑产影响，提高游戏口碑。

借助高质量第三方合作伙伴的能力

借助第三方合作伙伴，可高效以帮助游戏厂商构建更健全、更安全的经济系统，抵御复杂多变的风险，同时提升玩家对游戏内交易的信任和参与度。这种协作模式不仅是解决游戏内经济安全问题的有效方式，也是一种可持续的长期战略选择，ACE当前也向全球游戏厂商提供此服务。

方案支持：

HTTPS接口接入，任意端均可支持

安卓 iOS windows 小程序游戏 页游 国内游戏 国内厂商出海游戏 海外游戏

03. 内容安全问题的应对

跟其他平台的内容安全问题有所不同，游戏内的内容安全问题除了包含常见的违规内容风险外，还有特定的游戏类内容安全问题。在腾讯游戏安全与反网络黑灰产联盟联合发布的《网络黑灰产问题处置指南》中，腾讯游戏安全和联盟也对此类问题的应对做了相应建议。

建立违规信息防控标准

为提升运营方对违规信息审查的效力，可制定新游戏上线接入违规信息检测安全技术方案并接入红线标准，包括检测能力标准、处罚能力标准、人工审核能力标准以及产品功能形态标准等。

实施源头风险控制

包括但不限于：游戏数据分析、设备信息本地化检测 、异常行为监测等，从违规信息源头进行风险控制，以便及时发现并处理潜在违规行为 。

加强用户防诈骗教育

在产品内外官网论坛等适合场景设置防诈骗公告，滚动提示用户注意防范。通过积极引导提高用户的自我安全意识和防诈意识，帮助其了解相关法律法规，避免遭受欺诈行为的伤害。同时，鼓励玩家积极抵制破坏发言环境的行为。

优化突发事件舆情管理

运营方应建立完善的重大或突发事件预警响应机制。当重大事件发生时，各团队和部门需具有快速制定相关标准并高效部署最新违规信息检测能力。同时还需要合理配置人工审核资源，并设立专项数据监测以保障网络发言环境的和谐稳定。

建立违规信息检测机制

运营方应建立健全用户注册、账号管理、信息发布实时审核、跟帖评论审核、实时巡查、应急处置和网络谣言、黑灰产业链信息处置等制度，高效准确识别出违规内容。

实时阻断与处罚

一旦检测到违规信息，运营方应立即采取措施进行实时拦截，有效阻断违规信息曝光及传播。根据法律法规及设立的相关处罚标准，对发布违规信息的账号予以禁言或封号处理，避免对正常用户造成干扰，净化网络空间环境。

腾讯游戏安全方案

目前，腾讯游戏安全凭借多年在游戏领域的深耕，同样已经建立了一套专门针对游戏的内容安全方案，并且适用于国内和海外游戏，**现已向业界提供安全方案，欢迎联系免费试用。**

A 文本审核

腾讯游戏安全的内容安全方案，基于深度学习技术，可以检测和识别文本中包含的敏感、色情

低俗、辱骂、暴恐等恶意信息，对于游戏内特有的游戏业务广告、拉人信息，以及DIY建造场景内的恶意内容等也能够做到精准检测，有效规避游戏风险，保障玩家体验。

B 图片审核

传统（头像、聊天等）图片检测上，基于机器视觉图像处理技术，能自动检测图片，识别涉黄、涉恐、广告等违规内容，同时结合OCR识别、非法二维码识别、马赛克检测等，达到更精准的识别效果。支持图片相似度拦截，打击自定义的违规图片。

C DIY图片审核

基于ACE图片审核大模型开发了DIY垂类大模型，对于放置、摆放、搭建、建造和涂鸦等游戏特色建造玩法，均有针对性的审核方案。涵盖了建造文字、建造政治图标、性相关、枪支武器图形等内容，同时支持建造坐标审核和地图截图审核，可检测DIY中多见的涉政、色情、广告、惊悚、血腥违规类型。结合ACE的后台系统，可以实现先机审后人审，灵活控制推审比例，既减少了玩家的创作等待时间，也降低了人工审核的成本。

D 语音审核

审核能力持续升级，已有关键词检测模型、音转文模型、声纹模型、色情娇喘声模型、语音大模型等，支持对不同违规内容的检测，并兼容业界常用的语音格式。同时，区分语音流与语音消息场景，更加贴合游戏不同语音场景的安全需求。

E 策略定制

方案支持恶意子类型的选择，可个性化定制符合游戏的过滤策略组合，并支持自定义关键词及图库的管理，有效对齐游戏拦截标准，防止引流广告、低俗信息、地域黑、其他违规广告等的侵入。

F 运营平台

基于腾讯数百款游戏运营经验，搭建了适合游戏领域的内容安全产品化平台，涵盖场景管理、策略运营、人工审核/标注、回溯等功能，覆盖游戏运营全流程。

截止至2024年底，腾讯ACE内容安全方案适配的语言类型

英语	葡语	中文	泰语	越南语	阿拉伯语
意大利语	印尼语	韩语	俄语	日语	法语
西语	德语	土耳其语	波兰语		

方案支持：

HTTPS接口接入，任意端均可支持

安卓　iOS　windows　小程序游戏　页游　国内游戏　国内厂商出海游戏　海外游戏

04. 账号安全问题的应对

账号安全对抗是一个典型的符合“木桶原理”的场景，即如果存在短板，则黑产必然会出现利用短板的攻击。在账号安全的方案建设上，需要确保登录前、登录时、游戏中等全过程中无漏洞，全链路都需要有完备的安全保证。

登录前

登录前，确保登录协议无漏洞，如不能被劫持篡改、模拟登录等，防止被批量撞库和拖库

登录时

登录时，需要尽可能确保用户客户端环境安全，做好客户端防御

游戏中

游戏中，可以对游戏环境做进一步的识别，在获得用户同意或授权的基础上，结合游戏日志的历史记录做匹配

其他注意事项

同时可采取以下方式最大限度保护游戏玩家账号。

构建全面的安全防护体系

游戏厂商与安全公司等第三方机构合作，共同打击钓鱼网站、黑客攻击等威胁，构建全面的安全防护体系

加强法律手段的运用

对于那些侵犯用户账号安全的行为，游戏厂商应积极利用法律手段进行打击和防范，包括但不限于移送立案调查、提起法律诉讼等。

账号被盗前中后期的注意事项

与此同时，针对账号被盗问题，游戏厂商应当以预防为主，防治结合，在被盗前、中、后制定相应应对方案

被盗前

增强用户教育与培训：游戏厂商应通过各种渠道，如游戏内公告、邮件、官方网站等，教育玩家如何保护自己的账号安全。

增加玩家主动防护账号安全能力和风险提醒。

被盗中

及时全面识别盗号实施过程，并制定有效阻断方案。

提供多因素身份验证：游戏厂商应该提供多因素身份验证（MFA）作为用户账户的默认设置。

■ 被盗后

合理设计账号恢复机制：当玩家的账号被盗后，如何迅速、准确且安全地恢复账号对于保障玩家权益至关重要。

联动客户端+后台策略，准确有效的还原被盗事实，为被盗恢复提供确切依据。

05. 游戏DDoS攻击的应对

对于游戏厂商来说，DDoS攻击是一个常见且严重的威胁，腾讯游戏安全联合腾讯安全推出的游戏DDoS防护方案，通过充足、优质的DDoS防护资源，结合持续进化的“自研+AI 智能识别”清洗算法，保障用户业务的稳定、安全运行。我们对游戏厂商在应对此类问题时，也提出以下措施进行有效应对：

风险评估和巡检

与此同时，针对账号被盗问题，游戏厂商应当以预防为主，防治结合，在被盗前、中、后制定相应应对方案

安全风险评估

在游戏上线前，借助专业的安全扫描工具，对服务器操作系统开展全面排查。着重检测诸如缓冲区溢出、权限提升这类高危漏洞，从系统底层筑牢安全基石。针对游戏应用程序进行安全风险评估，确保应用程序不存在逻辑漏洞与注入风险；同时，进行风险评估，评估DDoS攻击可能对业务造成的影响，以便提前做好准备。

常态化巡检机制

在日常运维过程中，部署专业的网络流量分析工具，持续收集网络流量数据，从而构建精确的正常流量基线模型，并科学合理地设定异常流量阈值。一旦网络流量出现异常波动，例如短时

间内流量急剧上升，或者特定端口流量表现异常，系统能够即刻发出警报。同时，实时监控网络中频繁端口扫描、异常登录尝试等可疑行为，通过常态化的巡检监测机制，及时察觉并处理潜在风险，将 DDoS 攻击的隐患消除在早期阶段。

高效应急响应

智能流量清洗

当系统检测到 DDoS 攻击时，迅速启动将流量引导至清洗中心，清洗设备运用深度包检测（DPI）和机器学习算法，能够在海量的网络流量中精准辨别正常流量与攻击流量，保障正常流量能够顺利抵达游戏服务器，有效阻断攻击流量对服务器的冲击，维持游戏服务的基本运行。

智能流量调度

配置专业的内容分发网络（如 CDN），在游戏服务器前端部署节点，并对游戏静态资源进行缓存。当遭受攻击时，CDN 网络发挥强大的分流作用，将攻击流量均匀分散到各个节点，极大地减轻游戏服务器的压力。同时，根据攻击的实际情况，实时动态地调整缓存策略，进一步增强应对 DDoS 攻击的防护效果，降低攻击对游戏服务的负面影响程度。

多团队协作

跨部门应急团队

组建跨部门应急响应团队，网络安全专家剖析攻击态势，识别攻击类型、规模及潜在攻击源；运维工程师依据防护策略迅速调整服务器配置，保障稳定性；游戏业务人员协助评估攻击对游戏业务的影响范围和程度，为防护策略提供贴合业务的建议，确保应对措施有效实施。

高效协作流程构建

制定清晰协作流程，攻击发生时，监控部门及时传递信息给网络安全专家，专家制定策略同步

给运维和游戏业务人员。运维工程师执行配置调整等操作，与服务提供商协同；游戏业务人员评估业务影响并反馈。攻击缓解后，团队复盘总结，完善协作流程和应急预案，提升协同作战能力。

第三方服务团队支持

腾讯边缘安全加速平台（Tencent Cloud EdgeOne）

制定清晰协作流程，攻击发生时，监控部门及时传递信息给网络安全专家，专家制定策略同步给运维和游戏业务人员。运维工程师执行配置调整等操作，与服务提供商协同；游戏业务人员评估业务影响并反馈。攻击缓解后，团队复盘总结，完善协作流程和应急预案，提升协同作战能力。

A 防护“强”

边缘安全加速平台构建了网络层、传输层和应用层全方位立体防护体系。在网络层和传输层，EdgeOne 与全球主流网络运营商深度合作，依托海量优质网络资源，结合持续进化的"自研 +AI 智能识别"清洗算法，高效抵御各类 DDoS 攻击威胁。在应用层防护领域，EdgeOne 凭借领先的自研智能识别技术和精准人机挑战算法，配合高度灵活的精确匹配机制全面支持多元化业务场景下的访问控制与管理，精准识别并无缝拦截可疑和恶意请求，为业务构筑安全屏障。

B 服务“广”

边缘安全加速平台覆盖范围广，全球布局3200+节点资源，其中国内节点数2300+，海外节点数900+，单节点存储容量可达到40 TB~1.5 PB，带宽负载可达 40 Gbps~200 Gbps以上，全球骨干专线带宽100G+， 储备带宽 200 T+， 可以处理2万亿的日请求量，峰值3000W+ QPS，为不同区域的用户和游戏玩家提供高质量的就近安全和加速资源，实现本地化安全防护和加速。

C 下载“快”

边缘安全加速平台提供了CDN数据缓存和加速功能。 当客户数据需要更新时，可启动预热的功能， 将数据提前发布到中间源以及边缘节点，一方面极大提升了下载速度，提升用户下载感知，另一个方面也规避了大流量数据访问对源站产生的冲击。

D 时延“低”

边缘安全加速平台采用边缘节点、区域中心两级架构，通过节点间智能路由与专项路径优化，进一步提升网络加速效果，可有效解决跨国回源链路质量不佳与回源慢的问题。还提供了多协议加速的能力，针对TCP、UDP、Http/Https、Quic、gRPC等协议做了深度的加速优化，大幅度降低访问延时。

06. 其他游戏安全问题的应对

由于演员、代练等游戏安全问题变得越来越隐晦，需要游戏厂商在玩家游戏行为分析上更加的细致和精准。腾讯游戏安全在治理游戏中的恶意游戏行为，有着一套成熟的治理体系，通过对环境游戏内恶意游戏行为发生的链路进行分析，更深度地挖掘行为诱因和行为特征，确保技术策略检测稳定基础上，通过产品运营方案降低恶意游戏行为对游戏内环境平衡性影响。

从技术和运营层面，在玩家对局中、对局后进行针对性的干预。

01 优质玩家运营

官方引导建立良性玩家群体，推动良性玩家成为主流，提升正向口碑

02 动机分析干预

分析玩家进行消极游戏行为的动机，尝试从设计角度对于玩家诱因进行干预

03 明确行为规则

明确定性玩家消极游戏行为类型，针对不同的消极行为，设计不同的运营手段

04 提纯举报来源

数据层面，通过玩家分析过滤无效举报。系统层面，优化设计，诱导玩家有效举报

05 优化策略覆盖

放宽送人头策略检测条件，提升策略覆盖将已定性的消极行为纳入处罚

06 优化反馈体验

从缓解玩家负面情绪的角度调整举报反馈

运营层			技术层		
局中局后	局中	局后	局中局后	局中	局后
局内干预	举报优化	内容运营玩家宣导	行为检测	言语检测	演员对抗

07. 加强AI技术在游戏安全方案中的应用

随着人工智能技术（以下简称“AI”）的不断发展，在游戏安全对抗中，有很多的场景都可以把AI技术应用于其中，一方面可以减少游戏厂商在人力上的投入，另一方面通过AI深度学习算法训练检测模型，精确的判定异常账号。下面以腾讯游戏安全为例，分享AI技术在游戏安全中都有哪些方面的应用。

AI可帮助检测作弊玩家

腾讯游戏安全对抗方案体系中，其中包括Replay对抗方案，Replay是记录对局内玩家服务端与客户端交互的数据信息。完整包含了对局内所有玩家的游戏行为数据，可结合播放客户端重现整个对局过程。

游戏安全对抗可结合Replay数据特性，在解析出玩家对局行为序列数据的基础上，借助深度检测方案实现玩家间像素级视野可见性数据获取，并通过深度神经网络算法进行模型训练和迭代优化，增强对主流作弊功能和恶意行为的高覆盖和高准确性的检测能力，从而使replay成为无需样本依赖的通用、实时并覆盖游戏各种可能的作弊功能检测的安全方案，对于未知样本，未知作弊，以及高权限作弊形成有效的压制力，腾讯游戏安全目前在Replay的应用上已经相当成熟，并取得了突出的作弊检测效果。

AI可帮助厂商发现未知外挂

传统的外挂检测方法往往需要人工定义特征，这种方法既耗时又可能因为人的主观因素遗漏重要特征。而通过AI深度学习等算法可以自动从数据中学习和提取特征，大大提高了检测的效率和准确性。同时，AI模型不仅可以检测出当前已知的外挂样本，还可以通过学习已知外挂样本的特征去预测潜在的和未知的外挂样本，并对此做出预警。

因此，AI可以帮助厂商发现未知外挂，自动提取外挂底层特征，提高外挂检测的效率和准确性。

AI技术可以帮助保护虚拟财产，检测账号异常登录

通过对游戏数据的分析和检测，AI可以识别出异常的交易行为，比如频繁的大额交易，或者反常的登录、交易地点等，从而提前预警，保护玩家的虚拟财产安全。

AI技术可以基于玩家的游戏数据，通过深度检测算法，识别出异常的登录行为。比如，如果一个账号在短时间内从多个不同的地方登录，或者登录行为突然发生了改变，AI都可以及时感知这些异常行为，然后立刻提醒玩家，甚至可以自动锁定账号，防止账号被盗。

AI可以帮助检测经济类黑产群体

AI技术可以帮助游戏厂商有效应对黑产行为。通过数据分析和模式识别等技术，AI可以识别出黑产行为的特征和模式，并及时采取相应的对策。腾讯游戏安全的经济安全方案，就是从传统机器学习升级为深度学习，能更精准的检测黑账号及黑产交易，让游戏侧在对玩家账号、黑产交易进行处置时，有更充分的依据。

AI技术协助提升对违规文字、图像、语音的识别

在内容风控方案中，使用AI算法系统，采用深度学习和自然语言处理技术，对游戏中用于与其他玩家互动的文字、语音和图像内容进行收集和保存，能够自动识别包含恶意、辱骂、暴力等不适内容，并及时进行处理。系统通过大量的训练样本，让机器自我学习和优化，提高了信息审查的准确率和效率。

08. 建立玩家安全权益保障体系

参与行业标准共建

2024年8月，腾讯游戏安全联合中国计算机行业协会发布《移动游戏业务安全实施要求》，作为游戏安全行业的首个团体标准，该标准正式将"用户安全服务"以安全权益保障要求的形式列入游戏行业实行标准。标准构建了涵盖处罚权益、举报权益、账号及虚拟财产安全权益的三重保障体系，从全周期防护视角出发，要求游戏开发商、运营商、游戏安全服务商通过功能建设、运营管理以及技术保障等手段来确保玩家的基本安全权益内容。

以账号及虚拟财产的玩家权益保障为例，全生命周期中可施行的能力项包括：

■ **事前**

风险预警和应对	实时感知账号状态	保障号主控制权
异常提醒	登录环境和设备查询	身份验证

■ **事中**

账号和设备双维度登录验证	立即下线冻结	禁止财产流转
异常提醒 设备登录授权	冻结解冻	安全模式

■ **事后**

消除因被盗导致的违规处罚	找回被盗后流向系统的财产
被盗申诉	被盗找回

强化玩家安全权益认知

通过对典型场景进行数据分析，我们发现玩家在游戏安全权益上有更强烈的需求，特别是伴随着Z世代（1997-2012年出生）玩家占比的快速提升，年轻群体作为"数字原住民"相较前几代玩家更早形成安全意识，在安全价值主张，账号财产维权以及主动参与游戏环境建设等方向更为主动。具体来看，典型安全场景下的安全功能使用总量快速增长，2024全年同比增幅达20%，其中玩家主动使用规模占比近90%。这表现出该群体普遍对于个人安全权益需求敏感，有更强意愿了解和进行功能使用，需行业给予更多关注，如进一步构建和完善游戏玩家的自助安全服务体系。

升级处罚权益保障模式

伴随传统处罚证据体系的持续完善，以及处罚减免、申诉等玩家基础自助服务的覆盖，违规玩家的处罚权益得到保障。同时，基于行为限制解除和引导干预能力，处罚模式也在发生变化，其中行为限制以及通过干预可快速回归游戏等非传统处罚手段已占整体违规处置规模的39%。

伴随着"场景限制+行为干预"的规模化应用，干预对象的活跃、付费表现更佳，重复违规率平均可下降10%-15%。

建设玩家参与环境共建新能力

举报机制创新：建立复议机制，特别对于处理结果不满意等情况允许玩家主动发起新的处理流程，通过引入玩家众审/投票等手段进行二次评估，对违规者建立梯度化处罚校准机制，提升举报者的参与感和满意度。

账号安全：加强玩家自主防护意识，提供丰富的自助功能进行自我管理，覆盖从风险预警到被盗发生时的处理能力，以及被盗发生后快速挽回损失的全链路服务。

视频巡查：核心巡查员贡献巨大安全价值，典型业务日均处理可疑案例100万例，形成亿级正向安全口碑传播。

保障游戏营销活动及发货渠道安全

基于成熟玩家画像体系形成信用服务，围绕玩家核心关注的限量、限定、实价、可交易奖励类型， 在游戏内外、QQ/微信等各渠道的活动登录、参与、领取、发货等全链路部署信用防护能力，建立针对礼包商、羊毛党、黄牛党等黑灰产的信用对抗体系，年均阻断黑产非法获取活动奖励规模达数亿元。

目前，在黑产识别方面，腾讯游戏安全黑产识别模型已向业界提供：针对游戏产业中普遍存在的恶意打金、薅羊毛、恶意拉人、恶意广告等黑产行为，为游戏开发商、运营商以及其他游戏产业伙伴，提供游戏打金号、仓库号、点券金币商、资源商、礼包商、号商等游戏黑产角色的风险识别能力。接入使用方便，覆盖率、准确率高。

方案支持：

任意端均可支持，具体接入方式略有差别

安卓	iOS	windows	小程序游戏

信誉分服务升级为长期评估体系，持续激励优秀玩家

对影响团队竞技、破坏游戏公平、恶化社交环境的消极游戏行为，如挂机、恶意退出、消极对战、坐挂车、演员、辱骂等加大检测力度，通过匹配隔离、玩法限制等手段阻断或减弱违规玩家对游戏环境的影响；同时由"短期/实时信誉分"升级为"长期信誉分"体系，在严控重复违规率的基础上，增设绿色匹配专区、限定奖励、对局加成（经验值/道具掉落率等）等特权福利，持续激励保持健康游戏行为的优秀玩家。

中国地区关于游戏安全问题的法律法规

CHINA'S GAME SECURITY REGULATIONS

04.

中国对于打击外挂，维护游戏经济安全、内容安全等，提供了不同程度的法律支持，反映了中国对于保护知识产权、维护互联网健康发展的决心和态度，也侧面体现了游戏行业在法律层面上对抵制黑产行为的共识。

国家新闻出版署、国家网信办等部门曾多次开展专项行动，重点打击游戏私服、外挂等侵犯著作权的违法行为，净化网络环境。复制、销售、使用游戏私服、外挂等行为可能构成《计算机软件保护条例》下的"非法复制、传播、销售和使用他人已经注册登记或者未经授权的计算机软件、破坏技术保护措施"，可被公安机关处以警告、罚款等处罚。私服、外挂、黑产等行为，还可能妨碍、破坏游戏产品或服务的正常运行，从而构成《中华人民共和国反不正当竞争法》项下的不正当竞争行为，由此遭致最高三百万元人民币的处罚。并且，上述违规行为可能导致用户绕开实名认证、未成年人防沉迷等游戏行业行政监管要求。被侵权的游戏公司除可向有关部门投诉、举报外，还可以对黑产团伙提起诉讼，要求赔偿。

在此基础上，若相关行为情节严重，符合《中华人民共和国刑法》的定罪量刑标准，还可能涉及破坏计算机信息系统罪、非法侵入计算机信息系统罪、非法获取计算机信息系统数据罪、非法控制计算机信息系统罪，以及提供侵入、非法控制计算机信息系统程序、工具罪，或侵犯著作权罪等犯罪行为。

行业共建

INDUSTRY COLLABORATION FRAMEWORK

05

2024年12月

中国信通院发布第二期《数字安全护航技术能力全景图》，全景图展示了当前国内安全领域的众多品牌，其中腾讯游戏安全ACE凭借产品和技术实力入选全景图，在安全管理与运营、计算环境安全、密码技术与应用、数字安全服务、移动安全和应用与业务安全等6大安全领域18个子项目均有入选。

2024年12月17日

腾讯游戏安全联合《无畏契约》举办联合安全发布会，会上公布了一系列游戏安全举措，其中来自微软、高通、顺网、WeGame的专家发表讲话，指出正在与腾讯游戏安全联合共建游戏安全环境。

2024年8月22日

“移动游戏安全团体标准暨2024上半年游戏安全洞察报告发布会”在深圳召开。由腾讯游戏安全牵头，携手中国计算机行业协会、广东省游戏产业协会共同主办、本次会议发布了团体标准《移动游戏业务安全实施要求》及《2024上半年游戏安全洞察报告》，其中《移动游戏业务安全实施要求》是国内首个游戏安全领域的标准。

2024年8月21日

德国科隆国际游戏展 在德国科隆国际展览中心 举办，腾讯游戏安全亮相本届德国科隆展大会，作为领先的游戏安全品牌向全球游戏开发者展示了来自中国在游戏安全领域的先进技术方案。

2024年8月7日

腾讯游戏安全ACE接受了韩国最具人气和影响力的媒体之一——INVEN的采访，向韩国游戏厂商分享了ACE的反外挂经验。

2024年6月

腾讯游戏安全ACE的专家受到深圳大学“光明实验室”团队邀请，为实验室研究生开展人工智能算法专利实践经验分享。

2024年4-5月

腾讯游戏安全主办第九届腾讯游戏安全技术竞赛，该竞赛在武汉大学网络空间安全学院和华中科技大学网络空间安全学院支持下举办，共有2700多名高校学子参与。

2024年4月7日

腾讯游戏安全ACE接受了韩国最具影响力的经济媒体之一——《韩国经济日报》的采访，就“如何利用人工智能（AI）推动游戏安全技术进步 ”话题进行了讨论。

2024年3月

GDC2024（2024国际游戏开发者大会）在美国旧金山举办，腾讯游戏安全亮相本届GDC大会，作为领先的游戏安全品牌向全球游戏开发者展示了来自中国在游戏安全领域的先进技术方案。

2024年1月16日

由广东省游戏产业协会指导，腾讯游戏安全联合腾讯安全主办的第六届游戏安全行业峰会在深圳举办，峰会主题为主题为“守护游戏，公平竞技”。来自海内外的游戏安全专家在大会上做了分享，峰会吸引了50多家游戏厂商及上百名游戏行业从业者参与。

2024年1月16日

腾讯游戏安全联合广东省游戏产业协会、腾讯安全、伽马数据、DataEye发布了《20223游戏安全白皮书》，白皮书内容涵盖了游戏面临的安全风险与挑战、各类游戏安全风险的应对指南、中国地区关于游戏安全问题的法律法规、行业共建大事件、游戏安全对抗技术演变趋势与展望、全球典型游戏安全案例复盘等6大内容维度。

游戏安全对抗技术演变趋势与展望

SECURITY TECH EVOLUTION & TRENDS

06.

随着游戏安全方案的不断进化，游戏安全黑产也会不断演化，从早期的内存修改、代码注入，到现在的内核级别的攻击，游戏外挂技术已渐渐“深化”至操作系统内核层面，形成了一种“权限不对等”的安全对抗挑战。此外，游戏破解、账号盗取、虚假交易等安全问题也不断涌现。游戏厂商需要关注各类安全问题的演化趋势，及时找到有效的应对方案。游戏攻防技术的发展会与行业发展、技术进步和用户需求紧密相连，未来的发展趋势可以从以下几个方面进行展望

01. AI技术的广泛应用

AI技术将在游戏攻防技术中发挥重要作用。通过深度学习和机器学习算法，AI可以对游戏数据进行分析和建模，从而检测并预防作弊行为。此外，AI还可以通过对游戏数据的分析，提前预警和防止账号安全等问题。

02. 大数据分析的加强

大数据在游戏攻防技术中的应用也将加强。通过对大量的游戏数据进行分析，可以发现潜在的安全问题和异常行为，从而提前进行防护。

03. 隐私保护技术的提升

随着法律法规的完善以及用户对隐私保护意识的提高，游戏攻防技术也将更加注重用户隐私保护，确保获得用户的明确同意或授权，保证用户的个人信息权益。这将推动游戏开发商采用更先进的数据加密和匿名技术。

全球典型游戏安全案例复盘

GLOBAL CASE STUDIES

07.

过去一年，全球不同地区的热门游戏都不同程度出现了各类安全问题，以下，我们简要盘点了今年以来的典型游戏安全事件。

2024年2月

海外老牌格斗游戏高分排行榜遭遇外挂“刷榜”，高分玩家向官方倾诉不满

海外老牌格斗游戏游戏遭遇外挂攻击，游戏排行榜前列均被外挂玩家占领，多位高分向玩家向官方倾诉不满，认为他们的反作弊系统存在问题。

2024年2月

海外某MOBA游戏职业联赛遭受DDOS攻击，被迫给观众退票并改为录播

海外某MOBA类游戏职业联赛直播现场遭受DDOS攻击，导致赛事无法正常进行，赛事运营方被迫对现场观众进行退票处理，同时线上直播也改为录播。

2024年3月

某海外FPS游戏赛事直播现场，黑客入侵职业选手机器展示"自瞄、透视外挂"，玩家质疑游戏反作弊系统

某FPS游戏职业比赛直播现场因检测到使用”自瞄”和”透视”功能而中止比赛，事后赛事官方及给予的解释是因电脑被黑客入侵而导致出现了作弊行为。而这些作弊行为，已被线上线下多为观众看到，玩家对官方反作弊系统充满质疑。

2024年3月

海外某FPS游戏遭遇DDOS攻击，致使游戏客户端瘫痪数小时，玩家无法进行游戏

STEAM畅销榜第三热游，在上线几周内遭遇多次DDOS攻击，黑客们发现游戏防火墙弱点后，开始集中攻击游戏服务器，致使游戏服务器出现故障，玩家无法正常游戏。事后，厂商表示将成立反作弊团队来应对安全问题。

2024年3月

海外某知名IP游戏PC端上线仅30S就造破解，官方紧急对破解包进行处理

海外知名IP衍生游戏PC版在上线平台仅30S就遭遇，值得注意的是，该游戏并未采用防篡改技术，所以导致了游戏被快速破解。事发后，游戏官方对破解包进行了紧急处理。

2024年4月

某知名IP游戏出现BUG，玩家在游戏时会显示IP地址，多位玩家感到隐私被侵犯，给予游戏差评

某知名IP游戏出现重大BUG，玩家在游戏过程中会显示IP地址，游戏对手也能清楚的看到的IP所在地，这让多位玩家感觉隐私被侵犯，一时间多位玩家因为这个恶性BUG给予了差评。

2024年4月

海外某现象级游戏遭遇DDOS攻击，致使部分玩家无法登录游戏

海外爆火现象级游戏遭遇DDOS攻击，作弊者和黑客拦截了一批玩家登录官方服务器，尽管游戏官方有相应的反作弊措施，但仍未能阻止此类作弊行为。

2024年5月

海外某FPS游戏遭遇“无限手榴弹”外挂攻击

海外FPS游戏遭遇“无限手榴弹”外挂攻击，玩家对游戏的反作弊系统产生质疑。

2024年6月

海外某RPG游戏BUG十几年未修复，多平台游戏体验均受影响

海外某RPG游戏BUG多年未修复，多个平台上均出现此BUG：设备出现网络波动后，游戏将会进入未响应状态，待网络稳定后重启游戏，游戏进度也未能保存。据悉，该BUG已存在十几年之久，游戏官方仍未对该BUG做出回应。

2024年6月

海外某MMO游戏出现“物品复制”漏洞，大量复制道具流入游戏致使游戏经济系统受创

海外某MMO游戏出现“物品复制”漏洞，大量复制道具流入游戏，导致游戏经济系统受挫，因此不少玩家退游。

2024年8月

海外某FPS游戏遭作弊侵袭，核心指令遭破解

海外某FPS游戏遭到黑客攻击，破坏了游戏游戏内的关键指令系统，严重干扰了公平竞技环境，引发了全球玩家社群的广泛关注与热议。游戏开发商迅速响应，承诺将采取一系列强硬措施，包括但不限于升级反作弊系统、追踪并封禁违规账户，以及优化游戏代码以堵塞安全漏洞。

2024年8月

国产现象级单机游戏的火爆引发出游戏盗版、登录器热潮，导致诈骗案例数不胜数

国内某现象级爆款游戏的出现引爆游戏圈，相关的黑色产业也随之活跃，盗版游戏包、登录器代上号、贡献游戏账号等黑产服务纷纷涌现。一时间，真伪消息难以辨别，引发多起诈骗案例。

2024年8月

国产现象级单机游戏的火爆发布，STEAM平台遭受了DDOS攻击，导致玩家无法登录平台以及下载、购买游戏

国内某现象级爆款游戏发布之初，STEAM平台遭受了DDOS攻击，玩家无法正常登录STEAM平台，以及在平台购买和下载游戏。STEAM总体游戏的在线玩家数出现暴跌。

2024年8月

海外某FPS游戏仅一周时间内封禁超10000名作弊者

海外某知名FPS游戏开展反作弊清查行动，仅一周时间里，就有超过10000名的作弊者被封禁。其中 6,415 人被封禁账号 10 年，1,156 人被封禁设备/IP，而其余作弊者也被下发了不同程度的账号处罚。

2024年11月

海外某FPS游戏被黑客利用其反作弊系统，致使数千名玩家被”封禁“账号

海外某FPS游戏反作弊系统拥有自动识别机器人脚本关键词文本的能力，命中违规词的账号将会被封禁账号。而黑客利用该反作弊系统漏洞，向多名玩家发送违规文本，玩家查看消息后将会被封禁账号。目前该漏洞已被官方修复，被封禁的账号也已回复正常。

2024年10月

海外某知名RPG游戏遭遇”无限技能”外挂攻击，作弊者将外挂分享到玩家社区

海外某知名IP联动RPG游戏发布一周后，遭遇黑客攻击致使游戏内出现"无限技能"外挂，多名玩家被波及。后续外挂作者更是将外挂分享到游戏社区，进一步对游戏环境造成破坏，多名玩家通过退款的方式表达对官方的不满。

2024年12月

海外某知名RPG游戏发售不久便遭遇外挂“刷榜“，多名主播联名呼吁官方整治外挂

海外某RPG类型游戏火爆发售，在线玩家人数峰值超50W，随着游戏火爆，一些作弊玩家开始使用外挂占领天梯高分排行榜，多名主播公开分享他们与作弊者的遭遇，表达了他们对作弊行为的不满，同时呼吁官方整治外挂。

关于腾讯游戏安全

ABOUT ANTI-CHEAT EXPERT

08.

作为腾讯游戏的安全守护者，腾讯游戏安全团队已有20年游戏安全对抗技术和运营经验。目前，我们已经形成了一套完善全面，不断升级的安全服务，其中包括游戏反外挂、游戏加固、内容安全、游戏经济安全、数字版权保护等。

这套服务已经在腾讯运营的众多游戏和海量用户上得到验证，腾讯游戏安全也将持续携手游戏厂商共建游戏安全健康生态，营造更具公平性的游戏竞技环境。

欢迎关注腾讯游戏安全的官方微信公众号（腾讯游戏安全企业服务），及时获取最新的游戏安全干货。

相关单位

CONTRIBUTORS & PARTNERS

01. 指导发布单位

广东省游戏产业协会：现有会员单位近300家，涵盖所有的游戏细分领域及周边产业链，是广东省游戏产业领域极具影响力的省级行业协会。

02. 联合发布单位

腾讯安全：中国互联网安全新生态首倡者，由腾讯公司打造，以腾讯安全联合实验室作为实力技术支撑的网络安全领先品牌。腾讯安全以"一起，捍卫美好"为使命，致力于与客户、伙伴携手共进，追求卓越，全力守护数字世界美好未来。

伽马数据：伽马数据是中国权威的数字娱乐研究机构。作为中国音像与数字出版协会主管的中国游戏产业研究专家委员会的战略合作伙伴、数字IP应用工委秘书处单位，常年为游戏工委发布的《中国游戏产业报告》　提供支持和帮助，伽马数据(CNG)相关数据广泛被引用在媒体报道、券商分析报告、游戏企业研究报告。伽马数据(CNG)在数据领域积累了大量资源并沉淀了成熟

的研究方法，致力于以数据挖掘产业的发展特征，更好洞察产业未来的发展趋势，进而促进数字内容产业蓬勃发展。

DATAEYE：专注于全球数字化内容营销服务，跟踪全球游戏营销情报数据；研究全球游戏发行营销策略；

腾讯游戏安全：作为腾讯游戏的安全守护者，腾讯游戏安全团队已有20年游戏安全对抗技术和运营经验。目前，我们已经形成了一套完善全面，不断升级的安全服务，其中包括游戏反外挂、游戏加固、内容安全、游戏经济安全、数字版权保护等。

2024腾讯游戏安全白皮书

以下参编人员按姓名拼音首字母排列

白皮书参编人员:	蔡依然	陈旺林	程露萍
	邓立丰	邓　威	邓之珺
	丁　朝	董　硕	葛　浩
	龚承林	郭　晓	和　森
	何小龙	胡和君	黄金煌
	卢伟聪	贾新亮	江彩霞
	蒋卓立	李冠龙	李斯格
	李　鑫	李　云	李智威
	刘攀平	刘昱灵	马乐欣
	彭青白	乔　亲	舒卓卓
	孙国锦	王超力	王　翔
	王　钊	王哲君	魏　峰
	翁长军	吴晓翔	谢婧雯
	许锦福	杨玲亭	杨志宏
	尹潇涵	张仕雄	张　文
	张　旭	张玉璞	张子鹏
	赵　艳	郑　笑	钟芬芬
	周　杰	周志彬	
白皮书特别顾问:	陈　冬	董志强	李郁韬
	杨　勇	李长江	殷赵辉
	王嘉寅	王　岳	罗喜军
	王雅光	吴　昊	
人 员 鸣 谢:	邝蔚丹	孙冠绯	丰　华
	尹潇涵	滕　华	汪祥斌
项 目 统 筹:	李智威		

扫码免费体验游戏安全方案

扫码了解更多产品信息

关注【腾讯游戏安全企业服务】公众号