广东省游戏产业协会 × 网易智企 | 网易易盾

2023年度游戏安全观察与实践报告

全球游戏风险与合规治理趋势洞察

100亿+数据沉淀分析

1000+主流游戏安全痛点揭秘

10000+黑灰产工作室场景治理分析

前言

伴随着国内外游戏产业的高速发展，游戏安全问题正在成为影响玩家留存和活跃的关键因素之一。

游戏安全问题涉及诸多方面，比如影响游戏产品口碑与收入的游戏对战作弊与黑产工作室问题，影响游戏正常运营的未成年人治理、隐私合规以及内容安全问题等。

具体来说，游戏玩家为取得游戏内的竞争优势使用胜利借助作弊工具取巧。黑灰产工作室借助脚本工具疯狂掠夺游戏资源，破坏游戏经济生态，更有部分玩家以游戏为平台散播违规内容、拉人拉新等。

我们深知，游戏开发与运营者对建立游戏公平、绿色、健康向上生态的渴望。

为此，网易易盾一直致力于保护全球游戏开发者与运营者免受黑灰产工作室侵扰，保障游戏玩家享受公平的竞技环境，维护游戏互动社区绿色、和谐。

在过去的2023年，网易易盾基于游戏开发者通用型与定制化游戏安全需求，在通用解决方案上率先结合AI进行外挂与黑灰产治理实践。

本次《报告》将围绕游戏开发者与运营者常见的安全问题进行介绍说明，同时结合相关数据分析，展示在过去的一年中游戏安全相关的数据、问题与观察。

向游戏开发者与运营者展示立体、全面、系统的游戏安全知识与游戏安全洞察和实践。

卷首语

反网络黑灰产联盟

随着国内互联网信息技术的迅疾应用扩张和创新突破，基于经济利益诱导而自发形成的分工明确且衔接紧密网络黑灰产问题日益突出，游戏行业也深受相关黑灰产问题的侵扰（以下简称"游戏黑灰产问题"）。恶意注册、刷号养号、外挂、私服、非法账号租售、侵犯著作权、违规信息、网络暴力等游戏黑灰产问题已经演变成为企业正常经营过程中众多挑战之一。除了对用户和游戏业务方的正当利益造成损害，也会对产业整体环境的健康发展造成威胁，甚至可能会引发更加广泛的社会问题。因此，游戏黑灰产问题持续受到从业者们的密切关注，应对与处置刻不容缓。

网易易盾作为业内专业的服务提供商，持续深耕内容安全、业务安全、移动安全三大安全领域，致力于为游戏企业提供安全与合规解决方案，打击治理游戏黑灰产问题，是反网络黑灰产工作的参与者和践行者。《2023年度游戏安全观察与实践报告》详细介绍了游戏运营中存在的各类安全问题和治理实践，相信能为游戏网络黑灰产问题打击、处置及防范工作提供有效策略及解决方案，不断推动构筑健康、绿色、安全的游戏生态。

联盟也在此呼吁：应对和处置网络黑灰产问题需要社会各界的共同参与，希望有越来越多的力量加入到我们的队伍中来，集众智、汇众力，共同探索和寻求应对、处置网络黑灰产问题的最佳路径，实现对网络黑灰产问题的有效治理。

—— 反网络黑灰产联盟

2023年12月

"Ta 说"

游戏安全的首要任务是保证游戏公平性。通过强化技术手段打击外挂，以及黑灰产，以提升玩家的游戏体验和信任。

—— 程龙 网易雷火CTO

吉比特&雷霆游戏一贯坚持与侵犯知识产权行为作斗争，持续对市面上私服等黑产链条开展跟踪及定位，采用技术和法律手段严厉打击游戏私服、外挂等侵犯知识产权的行为。尽管私服经营者不断变换私服传播及经营方式，但吉比特&雷霆游戏协同警方亦在不断加强黑产监测手段，持续对私服等黑产保持高压打击态势，坚决为玩家维护健康游戏环境，决心与玩家携手共建和谐。

—— 易健 雷霆游戏 安全负责人

紫龙游戏在过去的经营中，坚持与侵犯知识产权的私服、破解支付协议、代充、游戏内打金、刷号工作室、游戏内聊天拉人等黑产灰产进行斗争，在这个过程中，黑灰产的人不断的变换方法，我们也随着这些变化不断调整策略进行分析和打击。在可以遇见的将来，由于这其中依然有很大的利润空间，这些黑灰产依然会不断的变换方法进行试探，我们仍将需要不断升级方法，把一些AI技术和合作伙伴的工具也用在里面，将他们对游戏的伤害，对玩家利益和我们厂商利益的侵蚀压缩在一个尽量小的空间，为玩家创造一个更加健康和谐的游戏环境。

—— 侯志芳 紫龙游戏CTO

游戏黑灰产工作室不仅破坏了游戏内的经济生态平衡，同时也影响了玩家正常获取资源的公平性。易盾通过技术监测游戏规则的执行，为我们《宿命回响》《灌篮高手》《航海王启航》等游戏在对抗黑灰产工作室作弊行为中提供了极大的帮助，从而营造一个公平、健康的游戏环境，让玩家能够享受到纯粹的游戏乐趣。

—— 陈永华 DeNA中国 游戏技术总监

“Ta 说”

《万国觉醒》作为全球领先的策略游戏，采用先进的反作弊技术和严格的账号安全系统，确保玩家的账号和个人信息得到有效保护。同时，《万国觉醒》通过持续的技术更新和规则完善，对黑灰产工作室、脚本外挂等进行监测和打击，为每一位玩家提供公平对战的游戏体验，共同守卫王国的荣耀。

—— 万国觉醒研发团队

《战意》一直将玩家的游戏体验放在首位，重视玩家反馈、优化玩家体验。特别是在游戏公平性，我们的运营团队本着绝不姑息在游戏中使用外挂、脚本等第三方非法软件玩家的原则，第一时间对扰乱游戏环境的相关玩家进行了封号处理。打造公平、健康、绿色的游戏对战环境是我们对玩家的首要承诺。

—— 《战意》运营团队

经研究表明，作弊玩家每进行一场游戏，不仅破坏环境，还潜在的对外挂进行了宣传与散播，大约1名作弊玩家每进行9把游戏，其作弊行为就会吸引1名新的玩家尝试外挂，可见作弊玩家是名副其实的毒瘤。因此，反作弊系统每进行一次升级，我们都相信这不是某种作弊行为的终结，而是与其进行持久战争的开始！我们会一直守望着玩家的安全游戏环境，并向大家及时同步我们的封禁与治理成果。

—— 王博 玩畅5E 游戏安全负责人

目录

2023年中国游戏安全风险概述

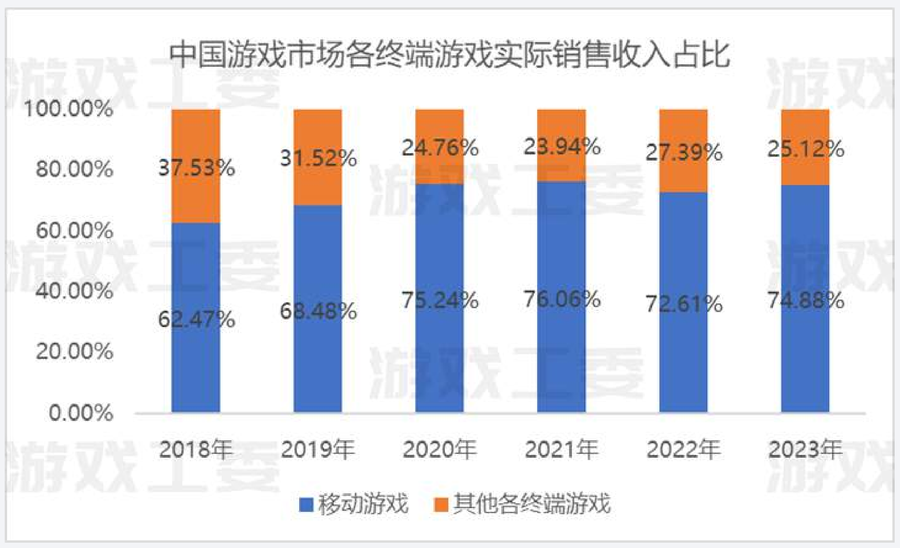
中国游戏市场规模

根据中国音数协游戏工委与中国游戏产业研究院发布的《2023年中国游戏产业报告》显示，2023年国内游戏市场实际销售收入为3029.64亿元，同比增长13.95%，并实现了首次突破3000亿关口。用户规模6.68亿人，同比增长0.61%，为历史新高点。

▲ 中国游戏市场实际销售收入

▲ 中国游戏用户规模

其中，国内移动游戏市场实际销售收入2268.6亿元，收入占比高达74.88%，继续占据主导地位；客户端游戏实销收入持续升高，占比21.88%；网页游戏继续萎缩，占比仅为1.57%。



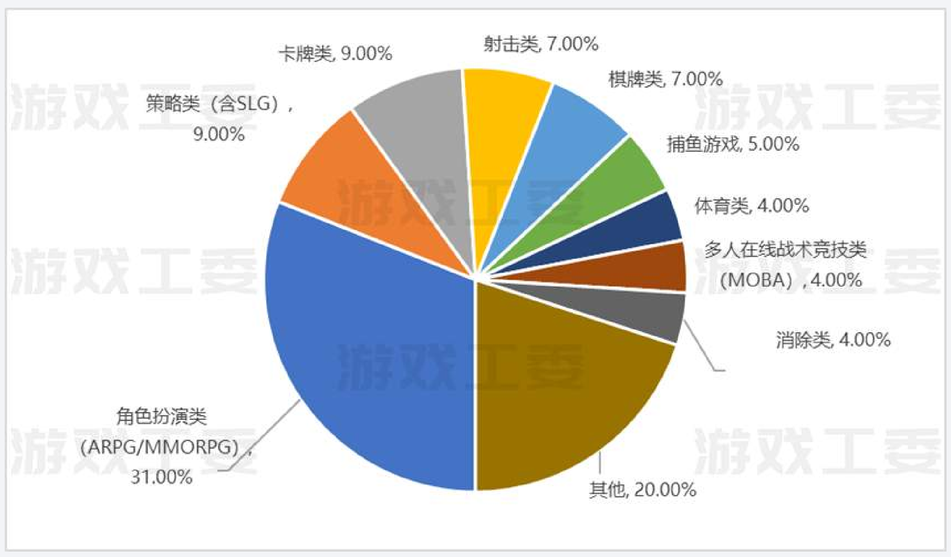
▲ 中国游戏市场各终端游戏实际销售收入占比

▲ 中国移动游戏市场实际销售收入及增长率

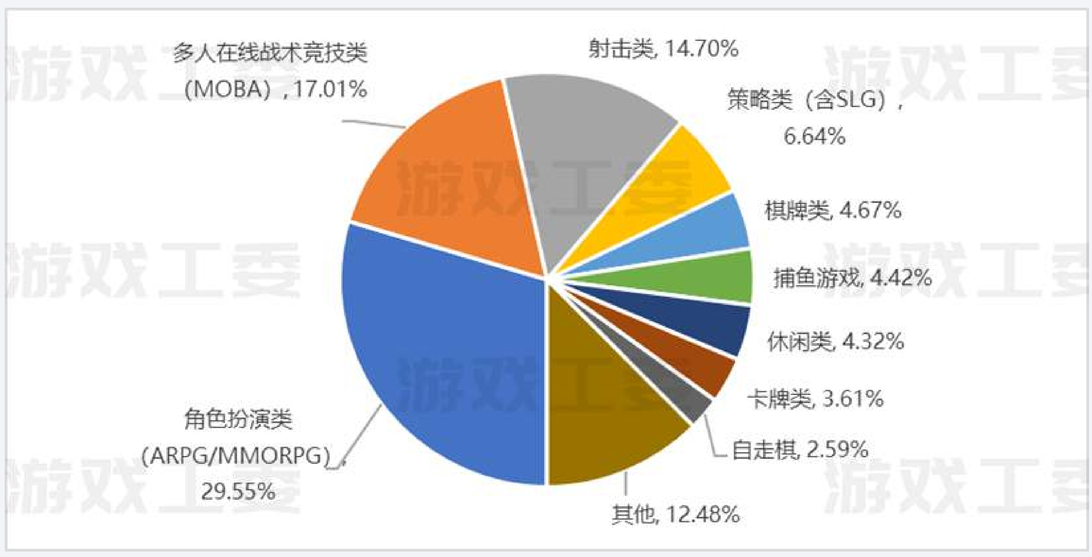
2023年中国游戏安全风险概述

以国内移动游戏市场收入前100位游戏产品为例，在收入方面，角色扮演类收入占比高达29.55%，位列第一，吸金能力可见一斑；多人在线战术竞技类次之，占比17.01%；射击类收入位居第三，占比14.7%。

在游戏类型方面，角色扮演类游戏数量明显高于其他类型，占比31%；策略、卡牌类数量占比分别为9%；射击和棋牌类数量占比分别为7%。



▲ 收入排名前100移动游戏产品类型数量占比



▲ 收入排名前100移动游戏产品类型收入占比

2023年中国游戏安全风险概述

中国游戏安全风险概述

2023年1-12月，国家出版署累计发放游戏版号1075款，其中国内版号977款，进口98款，国内数量较去年同期增长108.76%。整体来看，游戏作为国内最先走出"后疫情时代"的行业之一，取得了令人瞩目的成绩。

与此同时，游戏安全问题愈发严峻，纵观2023全年，游戏外挂与破解增多，网络DDoS攻击加剧，游戏内容安全、未成年人保护问题凸显，外挂制售产业链复杂演变等，都给游戏行业的健康发展埋下隐患。

1月，中国法院网披露江苏法院审理的网络游戏防沉迷系统破解案，犯罪分子通过非法获取公民个人信息和网络游戏账号的方式，规避、破解网络游戏的人脸识别程序和防沉迷系统，进而向未成年游戏玩家租售游戏账号牟取利益。

2月，Steam爆火游戏，由俄罗斯VK公司开发的《原子之心》被破解，这款国内售价239元的游戏，破解版最初由俄罗斯网站流出，且还是Steam豪华版，由此可见，俄罗斯黑客对自家公司也算毫不手下留情。

3月，湖北警方通报一起游戏外挂制售案件，广东某科技公司举报有网民制售《某游2》外挂程序，公安机关进一步侦办发现，犯罪嫌疑人通过QQ、微信等方式多次售卖外挂程序及游戏数据，涉案金额数十万。

4月，快快网络发布的《2023年DDoS全球攻击趋势专项报告》显示，互联网依然是DDoS攻击的主要目标，其中游戏连续四年在被攻击行业中占比超过一半以上，针对游戏的攻击很大一部分原因与竞品有关。

2023年中国游戏安全风险概述

5月，任天堂向Valve投诉即将登陆Steam的海豚模拟器，指责其为用户提供非法ROM密钥允许玩家随意模拟Wii和Gamecube游戏。任天堂的进一步声明表达了其对市面上所有第三方模拟器均持反对的态度。

10月，河北警方通报一起电信诈骗案件，犯罪嫌疑人利用某知名派对游戏中的聊天功能，通过低价售卖皮肤等话术诱导受害人下载第三方软件，进而实施电信诈骗。

网络游戏安全问题已随游戏行业发展"水涨船高"，重视并尝试解决游戏安全问题已成为继"游戏增长"之后，关乎"游戏产品生命周期"能否健康持续的最重要因素。

2023年网易易盾游戏安全检测概览

随着时代的变迁，游戏已经不是一项休闲娱乐工具，而是跃升为了一个包罗万象的社会形态。玩家在游戏中通过竞争与协作获取胜利，通过社交与互动获取同好，通过贸易与交易互通有无，它既独立于现实世界，又与现实世界密不可分。

正因如此，如果游戏内没有类似于人类社会的行为准则，那么人性中的"恶"便会被无限放大，比如玩家可以在游戏内通过各类工具获取竞争优势、攫取游戏资源，甚至发表不正当言论素材等。

网易易盾认为，围绕游戏影响游戏主体的不同，游戏安全主要包括：影响玩家个人/团队竞争公平性的外挂问题、影响游戏内资源分配与获取平衡的经济风险（黑灰产问题），以及破坏游戏内玩家社交健康的内容安全风险。

游戏外挂风险

游戏外挂问题一般指，游戏玩家为了取得胜利、获取更大的竞争优势，在游戏内使用脚本、外挂等辅助手段，从而破坏游戏对战平衡，获取非"正常"胜利的手段。

常见游戏外挂主要包括：包括修改器、模拟点击、恶意应用、加速器、盗版、私服、脱机挂等。

修改器	玩家通过脚本外挂可以改变游戏中的角色属性、游戏难度、资源数量、游戏界面等等。
加速器	使用外部软件或设备来提升游戏中角色的移动速度或操作速度的行为。
模拟点击	使用外部软件或设备来模拟玩家的点击操作，以实现自动化的游戏行为，如连续点击、释放技能、收集资源等。
恶意应用	使用恶意软件或应用程序，盗取用户的个人信息、账号密码，植入广告或恶意代码，甚至在用户不知情的情况下进行非法操作。
盗版	通过破解游戏的加密措施或获取游戏的非授权版本、服务器等。

2023年网易易盾游戏安全检测概览

网络封包挂	通过截取、篡改、重发或拦截游戏客户端和服务器之间的网络数据包，实现一些作弊功能，如卡配件、加速齿轮、看牌器等。
私服	通过窃取或泄露游戏后台服务器的代码和数据，搭建出一个非官方的盗版游戏服务器，可以让玩家体验到一些非正常的游戏内容，如神装、无限金币等。
脱机挂	通过逆向分析游戏协议，开发出一个非法的游戏客户端，可以脱离正版客户端运行，实现一些作弊功能，如多开刷副本、自动挂机等。

▲ 常见游戏外挂风险问题

游戏经济风险

游戏经济风险，主要指玩家及工作室商人利用自动化脚本低成本获取游戏内高价值的游戏币、道具、装备、点券等，从而破坏游戏内原有交易系统的价格体系和供求关系，以此导致游戏产生坏账、资源侵占、货币系统崩盘等。

常见的影响游戏经济问题的主要包括：打金工作室、脚本工作室、资源囤积号、渠道拉人号等。

打金工作室	通过开启大量角色重复刷取并囤积资源变现
多开工作室	一般为搬砖工作室较为常见，表现为通过V5多开软件突破多开客户端限制的用户（V5可以绕过技术检测）
脚本工作室	使用与该游戏玩法相关的辅助软件，完成一系列自动操作的用户 如自动登录、自动任务、自动采集等
资源囤积号	通过参与系统产出道具，通过第三方交易平台交易金币、道具等获利的用户群体，如初始号、自抽号、开局号
色情广告号	通过小号、租号等在游戏公屏或私聊他人发送垃圾信息引流至外部社区或APP获利

2023年网易易盾游戏安全检测概览

渠道拉人号	通过小号、租号等在游戏公屏或私聊他人发送垃圾信息引流至外部渠道获利
恶意组队号	事先与老板约定参与匹配玩法，帮助老板获取积分、荣誉、道具等获利，如押镖护卫号、代刷上分号，门童号

▲ 常见游戏经济风险问题参考

游戏内容风险

游戏内容安全风险，一般是指游戏内生产的内容不符合国家法律规定、社会公俗良德约束，以及恶意导流的相关文本、图片、表情、语音等。

随着沙盒游戏、派对游戏等开放世界游戏的发展，也衍生出了大量玩家自主创作的场景性违规内容，需要引起游戏厂商重点关注，此类问题轻者影响玩家体验，重者则会直接导致游戏停服危险。

游戏角色	主要指游戏角色的服装、昵称、面部表情（捏脸类）、角色摆拍等。
游戏场景	主要针对开放性由玩家自主创作的游戏场景。
游戏频道	包含世界频道、团队频道、队伍频道中发送涉嫌违规的文字、图片、表情、语音等。
游戏NPC	具备AIGC能力的游戏NPC，部分玩家引导NPC表达、表述非法内容。
游戏社区	游戏社区头像、昵称、备注等，同时发表相关文字、图片和表情。

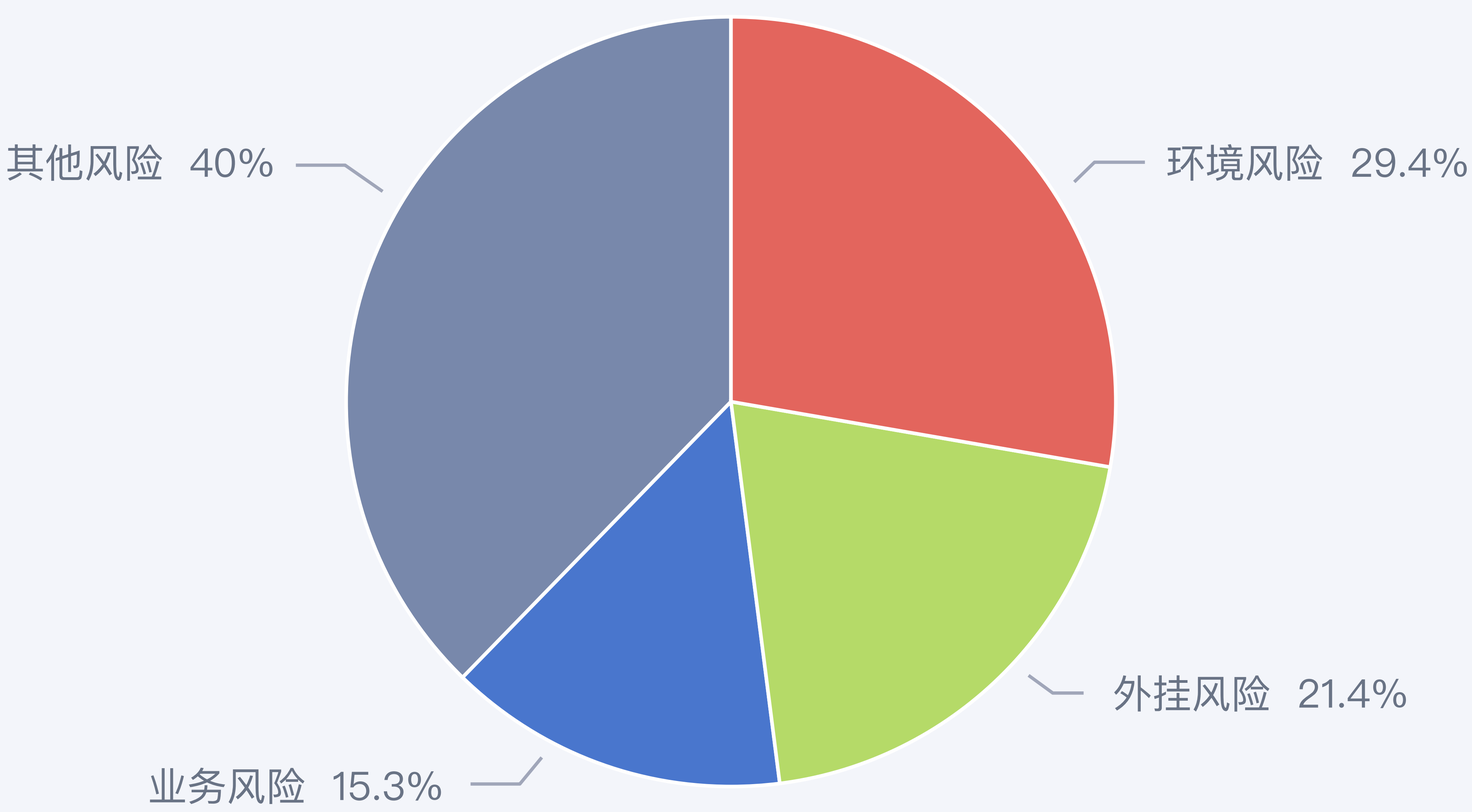
▲ 常见游戏内容风险问题参考

2023年网易易盾游戏安全检测概览

根据网易易盾游戏安全数据显示

2023年全年，游戏总体风险对抗激烈并呈现出上升态势，易盾全年累计检测安全风险217亿次，同比增长41.4%，其中环境风险威胁较大，检测63.8亿次，占整个检测安全风险类型的29.4%。外挂危险持续增长，2023年全年累计检测46.5亿次，占比21.4%，同比增长14%。

此外，本年度新增业务风险监测，全年累计检测37.8亿次，占游戏安全风险总体的15.3%。其他风险呈现出指数级增长态势，累计检测99亿次，占比40%，同比增长292.85%。

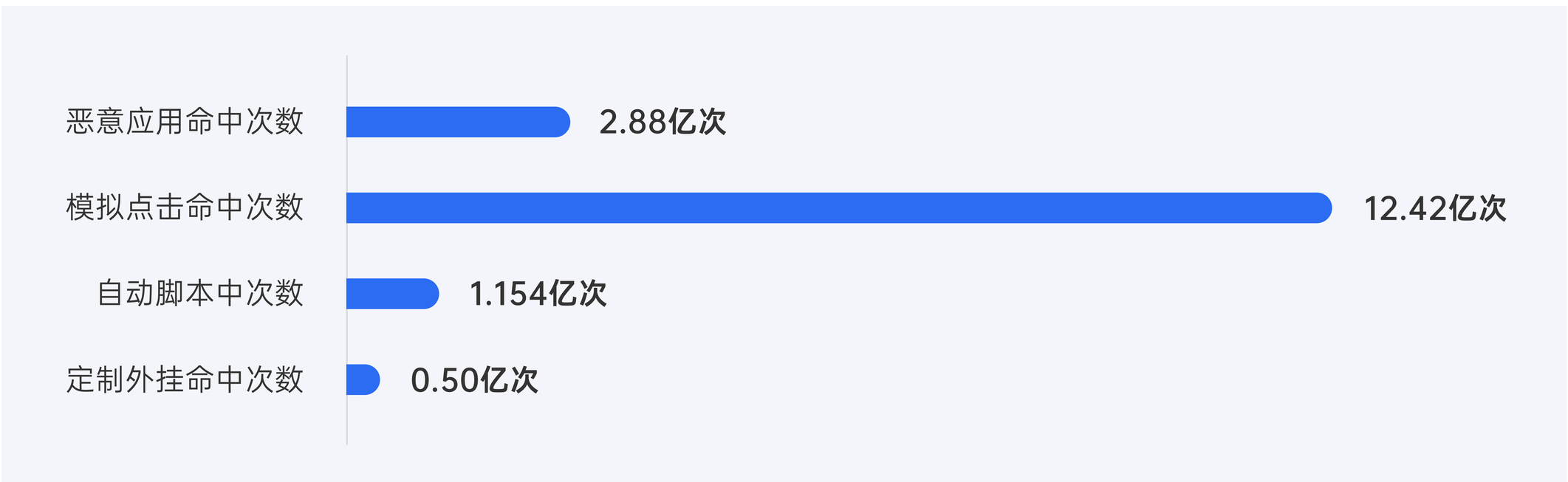


▲ 常见游戏内容风险问题参考

2023年网易易盾游戏安全检测概览

外挂风险

2023年，网易易盾围绕游戏外挂特征，通过定量分析手段，检测得出模拟点击类外挂12.42亿次，占比33%；检测恶意应用2.88亿次，占比7%；检测自动脚本1.154亿次，占比2.8%；定制外挂0.50亿次，占比1.3%。



▲ 外挂检测数据柱状图

在整个外挂命中数据中，手游外挂风险命中24.48亿次，占比66%，同比增长54%，端游外挂风险命中11.34亿次，占比31%，同比增长27%，此外小游戏/H5风险略有提升，命中1.8亿次，占比5%，同比增长90%。

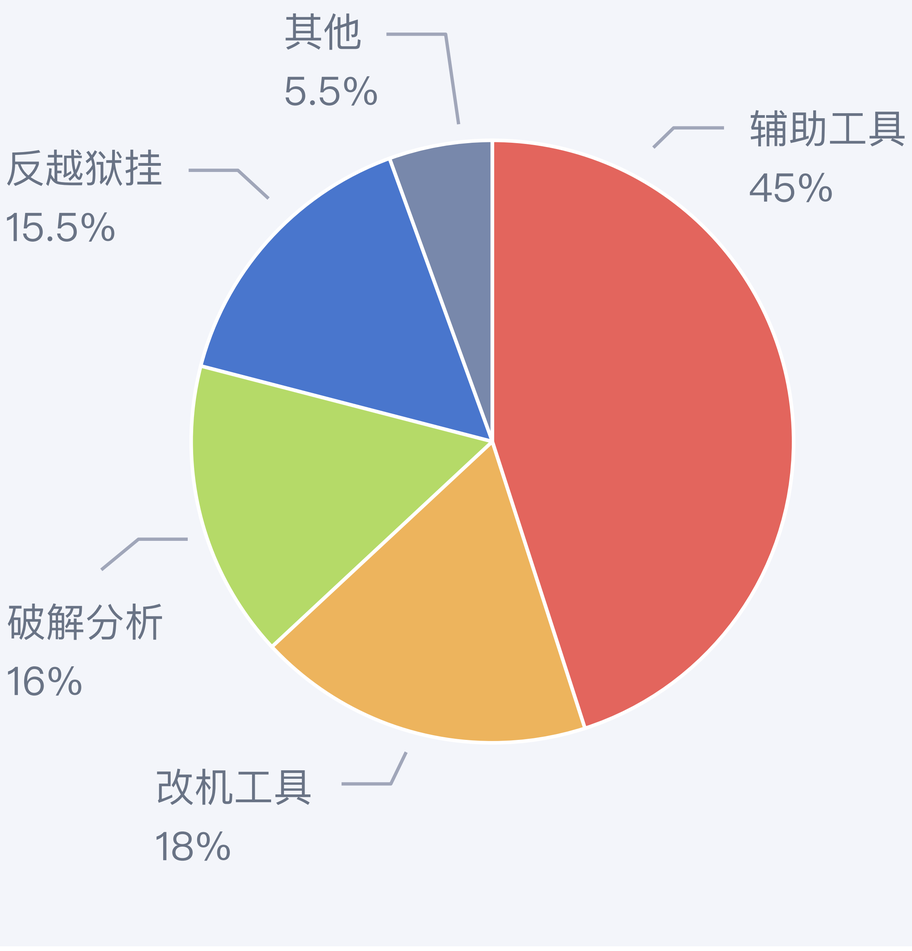
移动游戏外挂风险加剧

根据网易易盾2023年检测数据显示，网易易盾累计检测iOS终端受到攻击7.35亿次，安卓终端受到攻击17.13亿次，虽然两类都是移动终端系统，但是由于安全保护系统的区别，导致游戏外挂存在巨大的差异性。相比与iOS来说，安卓可以说是游戏外挂的重灾区，当然这也跟操作系统装机量有关。

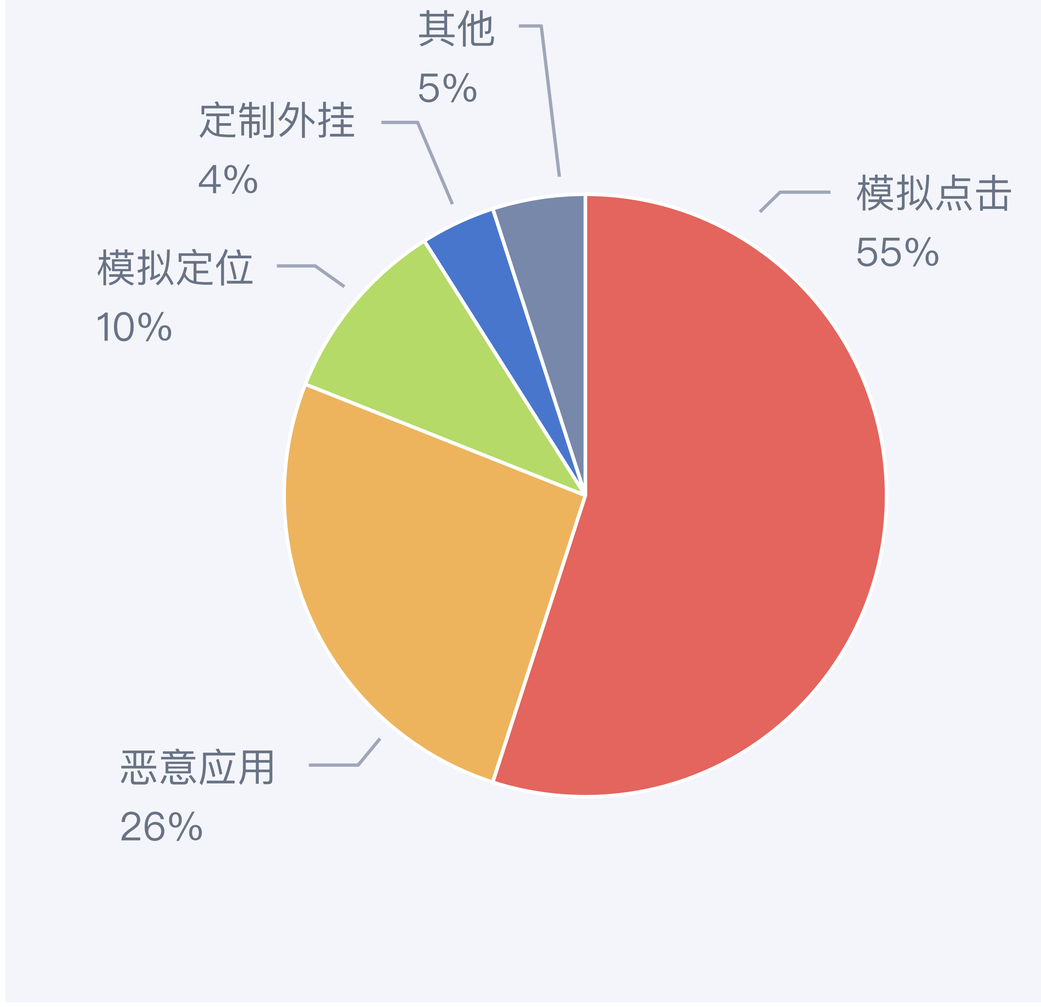
而从攻击方式来看，iOS和安卓也存在较大的差异，具体来说：

2023年网易易盾游戏安全检测概览

iOS手游受到外挂攻击前四的类型分别是：辅助工具、改机工具、破解分析和反越狱挂，占比分别为：45%、18%、16%、15.5%。而安卓手游受到攻击的前四种外挂行外为：模拟点击、恶意应用、模拟定位和定制外挂，占比分别为：55%、26%、10%、4%。



▲ iOS手游常见外挂占比



▲ 安卓手游常见外挂占比

网易易盾观察到，近年来，手游外挂和脚本工具越来越倾向于在非真机环境下运行，部分外挂为了躲避游戏方常规的检测，通常会使用隐藏安装和特征的手段对抗风控。

具体来说：

① 协议破解正在成为手游一大问题，外挂工具通过使用网络抓包工具如 Wireshark，抓取并分析游戏客户端和服务器之间的通信数据包，进而找出游戏客户端和服务器之间的通信协议，再通过模拟游戏客户端发送请求，以此获取或修改游戏数据。

② 在游戏支持断网的情况下，外挂也容易对本地数据进行修改，导致核心数据在断网后发生变化。

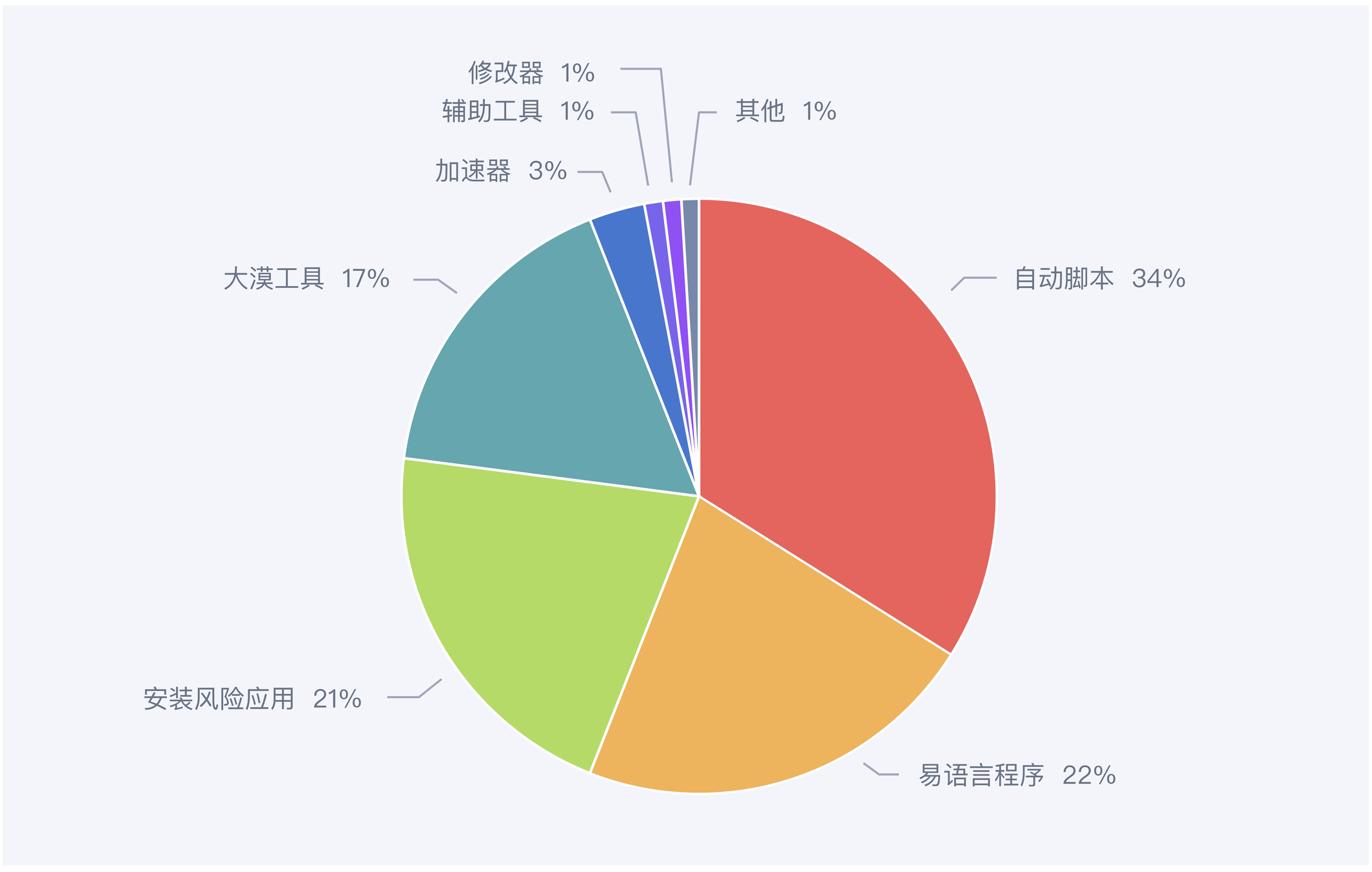
2023年网易易盾游戏安全检测概览

③ 跨环境作弊的现象也逐渐显现，即游戏包在模拟器内运行，而外挂则在PC端运行。比如按键类脚本和 CE 修改器等辅助外挂可以跨安装环境对手游下发作弊动作，而随着手游外挂检测和对抗手段的升级，这类作弊现象也呈上升趋势。

④ 剥离安全方案也是安全厂商和游戏方需要重视的问题，外挂通过屏蔽安全域名和截断通信的方式，实现外挂对抗方案剥离，给游戏方造成检测无数据的问题。

端游外挂风险

2023年，网易易盾检测端游外挂攻击类型中，占据前四的分别是自动脚本、易语言程序、安装风险应用和大漠工具，占比分别为34%、22%、21%、17%，而紧随其后的依次为加速器、辅助工具和修改器。



▲ 端游不同类型外挂攻击占比

2023年网易易盾游戏安全检测概览

此外，结合 2023 全年发现和监控到的端游外挂样本分析发现，超过30 % 的端游外挂都带有驱动注入功能，外挂开始向驱动层面发展，这也为外挂检测带来了更大的挑战。

我们也看到，与手游相比，PC端的外挂甚至可以做到一日多更，并且可以频繁、随机地修改名称、窗口哈希和 MD5 等信息。同时，有些外挂不仅直接下载在客户端，同时还会被放置在U盘、云端或网页链接上，使得检测难度更大。

同时，随着 AI 技术的发展，市面上现在出现了趋向AI行为的外挂。这些外挂在游戏动作执行上更加拟人化，不再僵硬，多应用于点击类脚本，售价也更高。这给AI模型的检测也加大了难度。

我们看到随着端游技术的不断创新，对抗外挂的手段也在不断升级。相对于移动端的安卓和iOS，PC端的运行环境更加复杂，权限更加开放，而端游的外挂治理也更为复杂。

小程序/H5小游戏外挂问题日渐凸显

近年来，小游戏市场需求的火热，伴随而来的黑产问题加速凸显。

根据网易易盾检测数据显示，网易易盾2023年检测小游戏类型来看，借助网络安全漏洞进行攻击和非法操作最为普遍，两者占比超过90%，因此网络安全漏洞是小游戏面临的主要威胁之一。

由于攻击者可以通过网络安全漏洞入侵游戏服务器或用户设备，获取敏感信息或者进行其他恶意行为。同时，小游戏可能存在代码安全漏洞，例如缓冲区溢出、代码注入等，攻击者可以利用这些漏洞进行攻击或者非法操作。

所以小游戏运营方需要需要采取相应的安全措施，包括不断加强网络安全防护、确保代码安全可靠性、加强用户数据保护等方面，以保证小游戏的安全性和可靠性。

2023年网易易盾游戏安全检测概览

外挂风险治理实践

冷兵器对战游戏

《战意》因其丰富多样，独具策略感的游戏世界吸引了海量的玩家，上线后很快被外挂制作方盯上——他们通过兜售不同的外挂攫取利益，影响游戏平衡，破坏正常游戏玩家体验。最常见外挂类型如：加速、增伤、回血、锁头、对游戏武将进行伤害微调、微加速以及数值修改等。

在外挂识别方面，网易易盾风控引擎综合玩家行为数据、设备数据、应用数据、网络数据等，识别游戏中出现的修改器、变速器、调试器、模拟操作、工作室等外挂工具/行为，并形成游戏外挂大盘，《战意》只需要通过后台就可以掌握游戏内环境动态变化，实现可视化数据管理。

小程序游戏案例

该游戏面临的主要问题是游戏美术资源被盗用、游戏数据被篡改。

其中，美术资源包括各类大场景、角色、道具等大量精美原创素材。此外，该游戏资源文件数量众多，需要保护的资源文件个数超过万个，这就要求游戏安全方案的加固性能、兼容性、安全性均需要达标才能符合游戏的需求。

易盾与游戏厂商充分交流后，结合该游戏特点，定制开发了游戏资源保护方案。保护方案支持png、jpg、js、html、json等格式游戏图片资源的加密，同时由于小游戏支持动态分包下发资源，定制方案也通过单独资源文件加密方式适配。

资源加密方案通过动态加解密的方式实现，可以有效对抗破解改包。资源加密方案同时在加固速度性能上做了特殊优化，确保游戏加固的时效，以支持厂商随时进行及时更新。

2023年网易易盾游戏安全检测概览

AI在反外挂中的应用与探索

随着外挂治理的深入，传统的反外挂方式不断被挑战， AI 在反外挂治理中正在逐渐发挥价值，特别是在解决客户特定痛点问题方面。

根据游戏品类的不同，使用AI解决的问题也存在差异，尤其是在对抗激烈或者收益颇高的场景中，作弊的花样也是层出不穷，但使用AI能够高效的针对作弊目的进行"反侦察"。

在MMORPG类型中的采集号、秒货号，通常使用AI计算点击行为作弊的玩家；在SLG的每日固定任务的场景中作弊玩家使用自动挂完成每日任务获取资源，AI在此场景中更多结合时间序列和操作动作识别出作弊玩家；在FPS对抗中，透视、自瞄和无后座，作弊玩家模拟鼠标信号，扰乱上报信息，一般厂商很难检测出作弊玩家，而AI在透视和自瞄场景中利用数据可以"还原"作弊的现场，不仅在检测覆盖率上解决了痛点问题，还能够提供可被查证的实质性证据。

当然，AI并不是万能的，需要和其他检测方案相辅相成，1+1>2。

据我们服务的客户经历来说，没有哪个厂商会轻易的将游戏终端"裸奔"上线，至少会购买我们的加固和风控引擎，或者客户自己实现了双端校验。

AI需要发挥的优势是基于数据，而数据可能是多源的，其中有来自游戏内的角色操作数据、移动数据等，另一部分来自客户端的输入数据或点击数据、或使用SDK采集的更细粒度数据，从而满足特定场景下的检测需求。

另外在检出结果上面我们会交叉验证作弊用户，提高处置着信息，在进一步分级将各自方案的边界逐步扩大，发挥出每个方案的优势，从而实现效果层面1+1>2的最高级别防控要求。

再比如在FPS场景中，AI的优势是辅助人工提高审核效率，在海量数据里面准确无误的检出作弊用户，但AI方案也存在边界，在业界最高标准里面几乎不可能做到又要准确率又要召回率的万能方案。所以在使用AI方案的时候应该明确好使用的侧重点以及想获得怎样的预期效果尤为重要。

2023年网易易盾游戏安全检测概览

经济安全风险

游戏黑灰产团伙概述

游戏经济安全主要以游戏黑灰产团伙为主，游戏黑灰产团伙是以游戏赚钱为目，通过多渠道，多手段，具备团伙性质的牟利群体。他们通常会使用自动化工具、同步器、多开器乃至脚本、外挂等作弊手段，通过大量重复刷取游戏资源实现获利，或以远高同等分段水平代替"付费玩家"实现上分的代练获利团伙。

该类团伙破坏了游戏交易交易平衡、冲击了游戏经济系统、影响了正常玩家体验，最终威胁到游戏本身的寿命与健康。

常见的游戏黑灰产团伙基本可以分成三个层级：

① 个体散户：一般以个人为主，通过较少的投资购置少量机器，基本靠人工手动，一旦碰到集体阵亡事件就很难翻身，抗风险能力差，危害一般。

② 中小型工作室：一般负责人通过雇佣几个员工看机器，依靠某一个或少数几个游戏项目，通过多开器、自动脚本实现获利，此类脚本在市面上流通广泛，抗风险能力一般，危害较大。

③ 工作室黑产核心圈：此类工作室规模庞大，掌握大量项目资源，由多个团伙组织结盟，分工明确，有专门的脚本研发供应商，该类脚本不在市面上流通，，抗风险能力高，危害极大。

游戏黑产工作室的第一优先级是有利可图，所以越来越多的厂商在设计游戏时就加入了很多反工作室的思想，例如资源无法交易、不常用设备风控等。

而工作室赚来的利润其实也养活了一个更庞大的黑灰产生态，为了便于理解，我们将其概括为：

① 与厂商风控团队对抗的上游：这些人很多时候并不了解游戏，反而对风控对抗比较有经验，如提供IP代理池与手机号池、虚拟定位技术、ROM改机定制技术、脚本开发技术等。

2023年网易易盾游戏安全检测概览

② 出售工具的第三方代理和配合工具落地的辅助平台的中游：比如专门出售外挂脚本的代理群主，专门销售改机工具的论坛和第三方交易平台，配合脚本持续运行的打码平台等；

③ 直接与用户对接的下游：其职权包含了游戏币变现、金本打手、游戏项目测试（哪些游戏存在获利点）、代练等，他们很多时候其实并不懂游戏作弊，甚至很多是兼职参与；

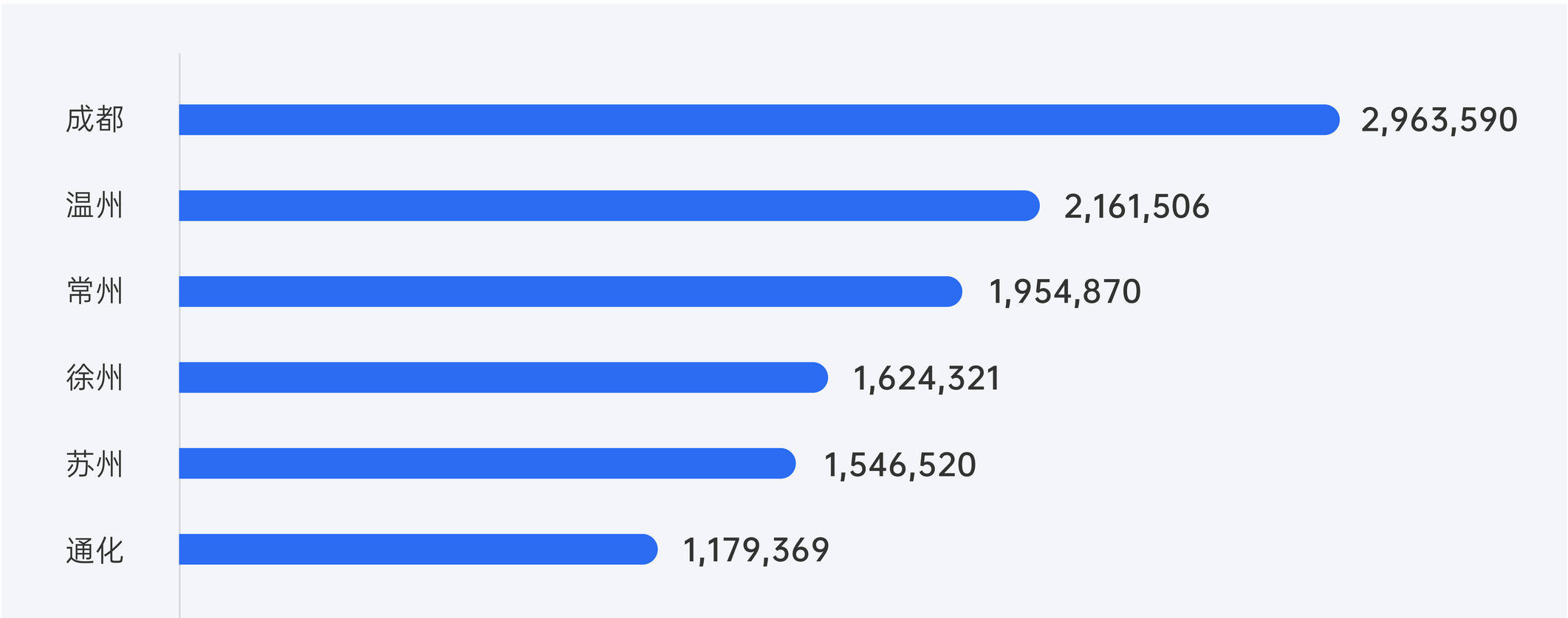
2023游戏黑灰产情况统计

在2023年游戏黑灰产攻击重点场景主要是围绕游戏充值、商城买卖、卡券交易、副本挂机等，在网易易盾黑产研究院进行深入研究后发现，工作室危害是所有黑产场景中最为猖獗的领域。

易盾黑产研究院2023年监测在活跃的游戏黑产工作室团伙设备141万台，识别检出团伙账号超过1300万个，累计检测超过9000万人次。同比去年提升30%，价值规模超100亿元。在如此庞大的流水线式黑产规模下，游戏黑产团伙工作室的问题使我们不得不重视。

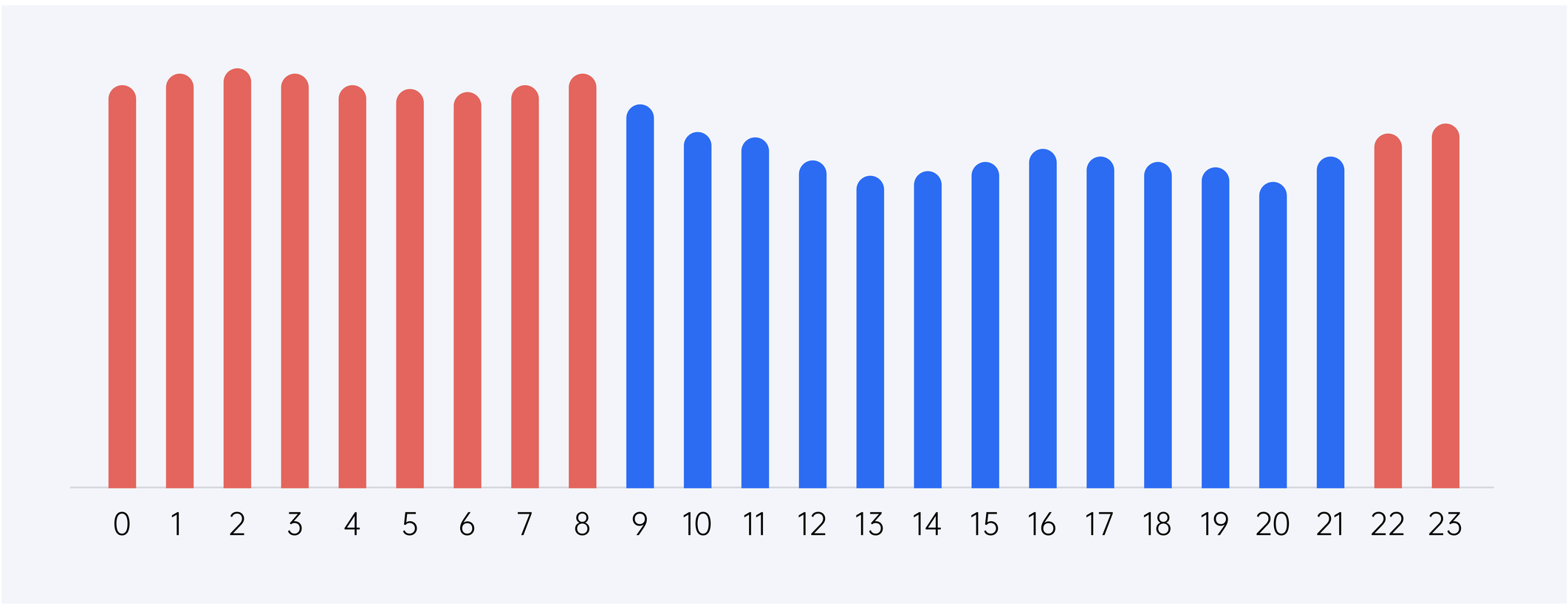
2023年网易易盾游戏安全检测概览

根据网易易盾安全部门检测，2023年国内游戏黑灰产团伙所在城市主要为成都、温州、常州、徐州、苏州等地，相比于2022年，温州、常州、徐州首次进入前5地区。同时，日本东京市、越南河内市与胡志明市为近年来首次进入游戏黑灰产团伙作案所在地top20榜单。



▲ 游戏黑灰产重点城市

游戏黑产工作室行动方式多以夜间为主，在对数以亿级的游戏黑产脚本分析发现，基本上游戏黑产工作室活跃的时间集中在晚上10点到早上8点为主。



▲ 黑灰产工作室脚本运营时间波动

2023年网易易盾游戏安全检测概览

黑灰产攻击场景分析

近些年，一些传统厂商已经开始学习如何利用数据分析完成多维度的策略输出，他们开始尝试从外挂脚本的目的出发，结合专家经验，还原游戏内的真实操作。

但在实际操作中，外挂样本多变且外挂作者采用A/B样本测试的方法，可以较为轻松地绕过多个规则或策略检测，同时许多工作室隐蔽性较强，存在故意创建新增角色麻痹业务方，让游戏厂商易于发现数据异常并疲于封禁，但是，真正成型的工作室群体却持续变现盈利，相当于给业务方释放一个"烟雾弹"。

特别是在新服或者大区首服节点，外挂表现更加明显。结合游戏黑产工作室渗透场景，游戏黑灰产主要渗透游戏以下几个板块：

账号类型	适用游戏	对游戏贡献	对游戏伤害	危害等级
初始号	卡牌类游戏，或具备抽卡、开箱类玩法的游戏	帮游戏吸引一部分的付费用户，购买初始号的群体都具备一定的付费能力	大批量的初始号导致普通用户不在游戏内进行付费抽取，严重影响游戏营收，对于正常抽取的用户属于不公平现象，影响游戏口碑	五颗星
首充号	具备首充机制且开放交易或类交易渠道的游戏	/	大批量刷取首充号，导致游戏币大量囤积，严重影响游戏收益，经济系统失衡	四星半
等级搬砖号	mmo类游戏	一定量的等级号可以稳定产品DAU和留存数据	大量的刷经验等级号占用服务器资源，严重影响正常用户，容易产生游戏负面舆情	五颗星

2023年网易易盾游戏安全检测概览

账号类型	适用游戏	对游戏贡献	对游戏伤害	危害等级
商人小号	所有开放交易的游戏	资源倒卖商促进活跃游戏内的交易系统，满足各阶层用户需求	返利商以及一些折扣元宝商影响产品营收	两星半
广告号/拉人工作室	开放聊天系统或可自定义文本区域的游戏	/	拉人影响游戏用户留存和收益	四星半
资源囤积商	slg	/	资源供大于求，物价失衡，影响游戏生命周期，给产品造成收益损失	五颗星
代练工作室	各类游戏和玩法	代练帮助付费用户解决游戏内繁杂任务，保障付费用户留存和付费收益	代练属于第三方渠道团伙，缺乏监管，容易造成被盗、开挂封停、危险言论等负面影响	两星半
打金牟利工作室	mmo类游戏，开放游戏币交易类玩法	打金工作室在游戏前期可以给市场供应一定的游戏币，如果游戏本身不出售游戏币，会满足老板大批量游戏币的需求，保障老板用户留存	大批量刷金游戏币导致原本游戏经济系统崩坏，物价失衡，影响普通用户收益和生存空间，导致用户大批量流失，如果游戏本身出售游戏币，会造成直接的收益损失	四星半

▲ 黑灰产工作室生态大盘

2023年网易易盾游戏安全检测概览

黑灰产工作室常用工具

多设备正常多开

通过多台设备来铺量，常见于小型工作室或散户，不挂载脚本，不注入第三方辅助，纯人工手动操作，游戏中常见的搬砖党。

第三方多开软件

单设备通过第三方软件，比如V5等PC端多开器，移动端自带多开功能的模拟器。

云平台和各类云手机

将云计算技术运用于网络终端服务，通过云服务器实现云服务，云设备或云平台实现大批量多开的场景。

虚拟机和虚拟空间

虚拟机指通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统。在实体计算机中能够完成的工作在虚拟机中都能够实现。pc上的VMware，为了保障多开性能，多数会采用xp系统，游戏窗口分辨率采用800*600， 手机上比较多见的如vmos（虚拟大师）、x8沙箱、光速虚拟机。

群控

群控软件是通过使用多部真实手机或模拟多部手机，通过跨端安装群控软件，下发脚本或是同步器操作控制手机上的 APP，达到模拟人工使用APP的效果，其目的是通过自动化手段，最大化模拟真实用户的操作请求。群控通常又可以分为线控、云控、主板机+群控软件3种模式：

① 线控：自己搭建服务器和实体手机，通过局域网内的连线操作实现一台电脑控制N个手机。

2023年网易易盾游戏安全检测概览

② 云控：不需要自己搭建服务器和实体手机，不受数据线地域的限制，手机一般是使用模拟器，手机安装云控助手，接收服务器发送的指令自动执行脚本，传输方面不如线控稳定。

③ 主板机：将多个手机主板去屏幕、电池集成到机箱中，采用独立的电源供电，可以一键开关机，配合群控软件（如来喜助手）实现群控功能。

常见黑灰产工作室管控方式

黑灰产工作室作为伴随游戏而生的一种衍生团伙，他们在游戏中不断吸收、蚕食游戏内的资源、金币、装备等，针对此类黑产工作室，游戏公司多采用角色踢下线、限制角色登录或者封号、玩法干预、限制交易，以及对收金老板进行管控等方式进行治理。

角色踢下线

该种方式为多数游戏厂商会选择的处理手段，主要针对多开数量超过游戏限定的游戏用户，对多开打击需求比较强烈且对及时性要求较高，执行踢下线操作，角色会退出到游戏登录界面。

角色限制登录或账号封停

通常又叫做封号，对违规的工作室角色限制登录一段时间或账号永久封停，这类操作执行手段严厉，对于工作室创伤较大，但是如果出现误处理情况也会引发负面舆情。

玩法干预

玩法干预主要是指针对打金牟利工作室做出的相对软性的处理机制，减少其在游戏内的获利比例，降低游戏方和工作室的直接对抗成本。

2023年网易易盾游戏安全检测概览

限制交易

对检测识别到的工作室群体进行标记，限制其在游戏内的所有渠道，所获得的游戏币和资源只能用于自身提升，该类处罚大大增加工作室的获利成本，容易后知后觉，减少工作室与游戏方的直接对抗，减少对抗压力。

收金老板的管控手段

对线下交易的收金老板号可进行收金管控，对线下的资金进行冻结，收金号需要从游戏商城购买同等的游戏币或充值同等价值的元宝进行解冻，减少游戏内线下交易的发生，从而压缩工作室的出金空间。

黑灰产攻击治理实践

某冒险格斗类游戏

该游戏类DNF的手游，这类游戏里的打金工作室比例非常高，且一直呈现出上涨趋势，网易易盾通过数据发现，游戏内工作室属于团伙批量起号，应该是属于打金囤号阶段。

针对该游戏打金工作室问题，通过玩法干预、账号隔离、预打击标记、账号封停、验证码弹窗等手段，保障该游戏DAU健康发展和经济体系稳定，在经过一段时间的治理之后，协同业务方对游戏内的打金工作室展开持续对抗，黑产占比从最高的50%下降至7%。

数字世界

数字世界是企业商业变现和建立客户互动关系的平台，但也被黑灰产团伙盯上。他们通过研究数字世界的产出和变现路径，并使用辅助工具模拟正常人的操作来获取收益。黑产工作室采用群控方式批量开启账户进行自动操作，以提高道具产出。他们通过交易系统将收益变现。黑产工作室行动专业化、规模化和有组织性，对正常用户获取资源造成失衡，影响数字世界的生态。外挂制作者为工作室提供辅助软件，并通过新媒体传播。外挂作者与普通玩家的公平性产生冲突，引发客户投诉和举报。

2023年网易易盾游戏安全检测概览

网易易盾通过智能风控和AI数据方案相结合的方式对抗工作室用户。个体用户通过购买物理按键作弊，而工作室用户则更多地使用按键类辅助软件。网易易盾使用用户行为检测和AI业务安全检测来识别作弊行为，同时结合风控方案进行治理打击。他们还采取了一些逃避检测的措施，如使用虚拟机、云手机、主板机等不同类型的设备。网易易盾使用AI模型在接收数据后进行毫秒级检测，并将结果反馈给业务方进行干预。在此过程中，网易易盾解决了辅助软件干扰和证据实时可视化的难题。

AI业务安全检测是通过分析和建模数字世界内的日志来识别群控工作室作为目标。网易易盾与该客户一起探讨玩法机制和高频沟通工作室形态变化，并基于数字世界上线了高适配AI数据方案。

- 第一种是基于用户主动操作行为构建的无监督方案，方案的优势是无论工作室群体如何变化，都能将相同操作的群体识别出来。

- 第二种是基于数字世界现实情况上线全场景全链路的用户任务时序方案，该方案优势在于高适配性数字世界场景，不仅支持群体用户实时检测需求，也解决了与历史用户相似性检索的新方案等。

- 第三种则是上线RMT检测方案，从交易变现环节识别工作室用户和倒卖群体的交易模式、交易途径等，常见的主流违规方式与游戏基本相似，如重复交易、不等价交易、抢货行为等。

AI在黑灰产治理中应用及前沿探索

AI不仅仅解决群体识别问题，还可以解决更复杂场景的问题

通过AI行为识别的应用和落地，可以使得厂商从更高维度上对篡改设备、云设备的识别中夺得了制空权，让工作室作弊的门槛和成本显著提高。也让厂商对自己游戏的生态和服务器健康程度有着实时的把控，将风险真正做到了预防和控制双管齐下。

2023年网易易盾游戏安全检测概览

另外，当游戏作弊的玩家通过真金获利时，群体的属性或边界变得模糊，如游戏中的代练、官方代打，天梯代刷、恶意开局、“买凶杀人”等复杂问题。比如，在官方代打场景中，玩家个人平时的操作和找专业工作室，两者在操作风格、技能熟练度、反应速度、打出效果数值等存在着明显的差异。

AI结合专家经验建立起不同层级的lab，再建立起有监督的方案，就能非常明显的定位出这些作弊的工作室。

AI方案同业务一道，始终准寻完整的牟利链路，将工作室的治理可控可测

无论是用AI方案还是业务规则方案，相同点是一样的，勾勒出工作室如何获利、如何变现、以及量化出获利的价值。当我们全面掌握了不同模式的工作室牟利链路，厂商在治理以及在后续和玩家的申诉中就占有绝对优势。

工作室的目的是逐利，用最小的成本获取最大的金钱收益。但不同游戏的差异我们不能忽视，AI方案的优势在于能像“剖丁解牛”那样游刃有余地适配各类场景。

虽然现阶段，越来越多的厂商拥抱AI，并不是追随时代的浪潮，更多的是降本驱动，但是借助现成不同游戏类型和场景的AI方案灵活组合，在黑灰产治理方面的效果将取得更好的效果。

2023年网易易盾游戏安全检测概览

内容合规风险

近年来，随着游戏产业的高速发展，游戏不仅成为了人们休闲娱乐了的工具，同时也扮演着文化传播的内容载体。伴随着开放式派对游戏的火爆，游戏内容创作不仅包含了游戏厂商的产出，同时玩家也在游戏内容创作中发挥着越来越大的价值。

同时，游戏具有极强的社交属性，游戏玩家在游戏中通过语音、文字、表情等形式进行团队配合、交友"唠嗑"、招募队友等等。

内容创作：创意也需要在规则内

在开放角色形象、场景等创作的游戏场景中，游戏厂商与玩家共同创作出了大量的内容，一方面好的创意被传播，另一方面一些违反社会伦理法律、暴力、色情、恐怖主义等不良内容也伴随而生。一旦内容被不法分子加以利用后则会很大程度影响游戏正向价值与持续运营，游戏企业不仅需要在内容创意上加强审核与审查，同时对于游戏内玩家创作内容也需要谨慎审核和审查，确保内容合法、合规、合理。

山川同异：重视文化风俗与地域差异

我国幅员辽阔，多名族混居，游戏内的场景、角色、服装等等应该尊重不同的地域风俗、文化习俗，同时弘扬文化繁荣。例如，在MMORPG、MOBA游戏中涉及的场景、人物形象、语音语料等应该尽量符合文化习俗规范，杜绝恶搞、挑衅等内容，避免违反相关法律法规。

社交聊天：言论自由不等于百无禁忌

游戏平台的社交属性决定了其自然而然会产生大量的社交内容，包括玩家头像、玩家昵称、玩家社群、互动聊天室、公共世界等。热门游戏和游戏社区很容易被某些玩家作为发泄情绪、散播谣言的主要阵地，游戏运营者不仅需要做好内容的监控，同时还需要做好实时的审核与治理。

2023年网易易盾游戏安全检测概览

拉人引流：热门游戏正成为拉新渠道

许多热门游戏由于在前期买量和游戏运营中投入了较好的资源，使得游戏玩家上量非常快。随着国内存量市场的竞争，热门游戏也会成为其他平台获取玩家/用户资源的一种渠道，他们通过在平台中发送相关的拉人、引流广告，引导玩家到其他平台试玩，而此类广告通畅又会有非常多的变种，较难识别，游戏平台如果不进行监管，则会导致用户逐步流失，进而影响游戏收益。

常见违规内容载体

游戏的垃圾信息包含多种多样，从形式上来看我们可以理解为文字、图片（含表情包）、音频为主，部分游戏内还存在视频载体内容。

文本内容：常规违规内容较多

文本内容作为最为常见的游戏互动载体，主要的违规内容包含色情、违禁、广告和谩骂，主要因为此类内容文本较为容易理解，且能够直接被其他玩家获取和感知。

文本内容会出现较多的变种类型，比如数字、字母、密码组合等，通过这种方式传播违规信息。

图片内容：视觉化素材更具冲击力

游戏内的图片类素材主要是以玩家头像、表情包和群聊内的.jpg格式图片为主，图片素材由于更为容易被理解且有传播性，所以图片类违规内容会增加更多的变形，比如二维码、恶心物、暴恐等，对于这类图片，游戏运营方需要第一时间进行处理封禁，特别是对于部分游戏允许自定义表情包上传。

音频内容：谩骂与色情占据主导

游戏的音频内容我们可以理解包含了游戏NPC语音、游戏动画语音、玩家单条语音，玩家实时互语音，相对来说最为常见的是玩家的互动语音，这类语音多见以谩骂为主，特别是在FPS游戏中，甚至一些团战类中，语音的谩骂较为常见。

2023年网易易盾游戏安全检测概览

违规内容治理难度

国内游戏中的违规内容由于涉及数量巨大，类型多样，更新快等特点，同时游戏违规内容又涉及各类监管问题，所以在治理难度上相对于其他载体更为困难，具体来说：

数量巨大

违规内容的量级很大，且影响的用户群体广泛。解决这些问题需要处理大量数据和信息，投入大量时间和资源。

类型多样

违规内容包括色情、广告、谩骂、违禁等多种类型，并且游戏场景也各不相同，因此针对不同的游戏场景和违规类型，需要采用不同的处理方法和技术，依赖高效精细的治理体系。

更新快

黑灰产常常采用文字变种、分段发布等方式，以绕开反垃圾策略，这使得平台需要持续攻防，增加了打击违规行为的难度。

2023年网易易盾游戏安全检测概览

违规内容治理建议

针对各类游戏内存在的内容风险问题，网易易盾内容安全团队在多年实践中积累了大量的经验。针对具体的游戏安全风险，网易易盾对于不同的内容载体进行了精细化的运营方式与拆解。

类型	问题	处理方式
文本审核	色情低俗、谩骂嘲讽、拉人引流	采用百万级别人工标注的游戏语料训练NLP模型，结合十万量级敏感词库能力，有效地检测和拦截内容中的色情低俗、谩骂嘲讽、拉人引流等有害信息
图片/视频审核	色情低俗、广告、违禁人物	采用上百个子分类CV模型，结合百万量级图库能力，可精细化检测拦截内容中包含的色情、性感低俗、广告、违禁人物等有害信息
语音审核	色情低俗、谩骂嘲讽、违禁人物	采用娇喘asmr、声纹识别以及ASR技术，结合违禁音频库，有效地识别音频中的娇喘呻吟声、违禁人物声音以及其他在文本审核中常见的违规有害信息

2023年网易易盾游戏安全检测概览

未成年人保护

2023年9月20日国务院第15次常务会议通过《未成年人网络保护条例》并公布自2024年1月1日起施行。

《未成年人网络保护条例》是我国第一部专门性的未成年人网络保护综合立法，《条例》规定网络产品和服务提供者应当及时修改可能造成未成年人沉迷的内容、功能或者规则，设置未成年人模式，每年向社会公布防沉迷工作情况。

特别是在网络游戏管理中，进一步明确网络游戏适龄提示要求，规定网络游戏服务提供者应当建立、完善预防未成年人沉迷网络的游戏规则，避免未成年人接触可能影响其身心健康的游戏内容或者游戏功能，并根据不同年龄阶段未成年人的身心发展特点和认知能力，对游戏产品进行分类。

在规范未成年人网络消费方面，规定网络服务提供者应当合理限制不同年龄阶段未成年人的单次消费数额和单日累计消费数额，不得向未成年人提供与其民事行为能力不符的付费服务。

建立健全未成年人保护机制

国家新闻出版署下发《关于进一步严格管理 切实防止未成年人沉迷网络游戏的通知》，针对未成年人过度使用甚至沉迷网络游戏问题，进一步严格管理措施，坚决防止未成年人沉迷网络游戏，切实保护未成年人身心健康。

《通知》要求各级出版管理部门要加强对防止未成年人沉迷网络游戏有关措施落实情况的监督检查，对未严格落实的网络游戏企业，依法依规严肃处理。

未成年人治理与保护并不是流于表面，而是需要深度理解游戏中对未成年人造成的伤害与价值观塑造。游戏公司应该建立起一套健全的审核机制，具体包括防沉迷系统、限制付费金额、互动内容合法合规等。

2023年网易易盾游戏安全检测概览

防沉迷系统

防沉迷系统旨在通过一些可识别的信息为手段，去鉴别是否该类游戏为未成年人创建角色或者游戏，比如身份信息、银行卡信息、手机号信息。

考虑到未成年人会使用父母、亲属，甚至网络购买他人实名账号进行登录游戏，网易易盾建议可以利用人脸比对、身份证对比等方式来识别游戏登录这是否为未成年人，从而限制未成年人游戏时间。

未成年人识别

未成年人保护除了在登录阶段以外，在玩家进行游戏过程中也需要二次的识别和甄别，比如游戏语音内的声纹、玩家聊天中的未成年人黑化，甚至上线时间段与特殊时间点等，以此综合判断是否为未成年人。

2023年网易易盾游戏安全检测概览

隐私合规

游戏隐私合规是指游戏开发者和运营商需要遵守相关法规和规定，保护玩家的个人隐私和数据安全。

随着游戏行业的发展，用户个人数据的收集和处理成为了一个重要问题。为了保护用户的隐私权益，游戏行业采取了一系列的措施，确保用户数据的安全和合规处理。

监管愈发严格

截至2023年12月，全国各监管单位（省/市通管局、工信部、省网信办）通报责令整改/直接下架累计达87批次，全国各地月均累计通报10次，累计通报责令整改/下架App数量达约1600款，因App隐私合规问题被通报企业数达1500+家 。涉及多个游戏应用及企业。

游戏隐私合规解读

游戏行业必须遵守相关的隐私保护法规政策，如《个人信息保护法》和《网络安全法》等。游戏企业要了解和解读这些法规政策，并制定相应的隐私保护措施，确保用户数据的合规收集和处理。

在游戏开发和运营中，涉及到了大量的个人数据，如玩家的账号、游戏记录、支付信息等，因此需要严格保护玩家的隐私和数据安全。

《网安法》第四十一条规定收集使用个人信息需要符合"合法、正当、必要原则"。特别是手游游戏厂商在收集使用个人信息时的"告知-同意"模式，明确告知数据采集的目的、范围和使用方式。此外，游戏厂商需要严格保护玩家个人数据的安全，采取必要的安全措施，防止数据被盗取、泄露、滥用等。而游戏玩家有权访问、更正和删除自己的个人数据，游戏开发者和运营商需要提供相应的服务和支持。

同时，游戏厂商需要设计和实施合适的隐私政策和用户协议，明确规定数据使用和保护的相关事宜，并尽可能简明易懂。

2023年网易易盾游戏安全检测概览

游戏隐私合规用户权益保护

游戏企业应完善和公开透明的隐私政策。隐私政策应包括数据收集和处理的规则、用户权益保护的承诺、数据存储和转移的安全措施等内容。游戏企业要确保隐私政策的易于理解和访问，提供给用户明确的选择和控制权限。

游戏企业应加强对用户权益的保护。在用户个人数据收集和处理过程中，要确保用户的知情权、选择权和控制权。游戏企业要设立用户投诉和监督机制，及时处理用户的投诉和反馈，并采取措施保护用户的个人数据不被滥用或泄露。

网易易盾实践

易盾移动应用隐私检测服务，基于权威个人信息保护政策文件，覆盖政策要求所有场景，实时同步，紧密贴合监管要求。覆盖隐私信息获取、传输、存储等各类场景的检测项，囊括9大方向，共计33个检测项，同时适用于Android、iOS平台。详尽的检测报告、代码级问题定位及专业的咨询服务，代码层级问题定位，专业的隐私整改咨询服务，使整改更加高效。易盾智能隐私合规检测三大模式，代码层级问题定位，专业的隐私整改咨询服务，使整改更加高效，支持三方API接口模式，SaaS模式，检测工具部署模式。

2023年游戏不同游戏安全风险

游戏外挂

随着外挂技术的不断演进，市场上对定制外挂的需求愈加明显。易盾游戏安全的分析显示，定制外挂在其收集的样本中所占比例已经超过了90%。舆情监测平台的数据也反映出这一市场的快速响应性，一些热门的定制外挂甚至达到了每半天更新一次的频率，以适应客户的不断变化的需求。这些外挂主要通过代码注入、hook接口以及硬件驱动等方式实现，使得它们的行为更难以被发现，从而更加隐蔽和类似于真人行为。

在FPS游戏等外挂泛滥的领域中，微调外挂尤其受到追捧，因为它们通过精细的调整游戏数据，以至于与正常玩家几乎无异，大大降低了被游戏公司检测系统识别的可能性。这种高度拟人化的外挂不仅造成了市场需求的激增，且价格居高不下，对游戏的公平性和玩家的游戏体验构成了严重威胁。

为了应对这一挑战，游戏开发商需要持续完善和优化其安全策略，开发更加精准的检测算法来识别和区分外挂行为，同时加大法律和技术层面的打击力度，以保护公正的游戏环境和玩家的合法权益。

游戏破解与防破解

盗版和破解依旧是今年游戏厂商的一大痛点，相对没有安全防护的游戏包体，破解的门槛较低；外挂作者在破解手段上，从易盾收集的破解样本上来看，已经可以做到绕过游戏签名或者伪装成正常的游戏签名；除了常规破解包体重新封包的手段之外，也有的外挂脚本从协议方面入手，通过抓包工具拿到游戏通信信息，对数据包解密后，修改相关关键信息，重新上传给游戏服务端，从而实现作弊。

2023年游戏不同游戏安全风险

游戏安全新能力

在游戏安全攻防过程中，内存修改是最为常用得作弊方式，由于市面上模拟器越来越多，以及对游戏的运行支持愈发稳定，内存修改由最初的移动端作弊发展到了高纬度的跨端修改作弊，这其中最常用的作弊工具是PC端的Cheat Engine，去修改在模拟器上运行的游戏数据，由于模拟器上游戏的逻辑数据通过Vbox虚拟化到R3层的PC内存数据，只需要修改对应的PC内存数据即可达到作弊同时配合Cheat Engine的高度灵活性，为这一跨端作弊行为的检测带来了很大的挑战。易盾通过自研专用的引擎内存陷阱检测方案去解决这一技术难题。

游戏坏账问题愈发严峻

游戏坏账问题主要是黑灰产团伙通过非法渠道盗用信用卡信息，通过给玩家/用户代充的方式进行变现，同时利用appstore小额直接发放商品的漏洞实现伪充值/购买，进而实现被盗刷卡主退款，导致坏账。

同时，黑产团伙以低价为用户提供充值服务的形式，吸引用户购买其充值服务，利用渠道存在的利差赚取利益，导致官方渠道用户流失、实际营收下降。

此外，黑产团伙通过技术手段，拦截、囤积支付凭证，并使用此类无成本的支付凭证为他人app账号充值，对于业务方来说，实际不产生收入，但是支出了会员权益、道具等虚拟商品，直接造成坏账，甚至可能涉及洗钱操作，有法律风险。

2023年游戏出海安全风险

游戏合规

国内市场竞争的日趋激烈，使得许多的游戏厂商将目光瞄向了海外市场，除了欧美、日韩等发达地区之外，中东、东南亚、南美也成为中国游戏厂商游戏出海必选之地。

相较于国内熟悉的市场环境，许多刚刚进入海外市场的游戏公司很难适应对应地区的相关法律和规范。面对一个陌生的市场，游戏厂商需要关注许多方面的问题，比如内容合规性、法律法规合规、文化适应性、用户隐私保护、付款安全以及区域合作等。

内容合规

内容审查是游戏出海中的重要环节，不同国家和地区对游戏内容的审查标准存在差异，因此需要根据当地的法规和文化习惯进行内容审核，以确保符合出海地区/国家的法规和文化习惯。

游戏内容涉及游戏LOGO、游戏宣传视频、游戏角色、游戏服装道具、游戏配音等是否涉及暴力、血腥、性暗示、政治敏感、文化禁忌等元素的审查。为了确保合规，游戏开发者可以与当地的合作伙伴或第三方机构合作，进行内容审核和修改，以满足当地市场的需求和合规要求。

隐私合规

随着各国各地区隐私保护意识的提高，很多国家和地区的隐私保护法规也在逐步完善和加强，隐私合规既是用户权益的重要组成部分，也是企业信任的重要基础。同时，隐私合规也是企业进入国际市场、拓展海外业务的重要前提。

国内企业出海不仅需要做好本国法律和隐私合规，同时还需要面临全球各国、各地区不同的数据隐私法规要求。

例如，欧盟的《通用数据保护条例》（GDPR）、美国的《加州消费者隐私法案》（CCPA）等重要隐私保护法规的要求。

2023年游戏出海安全风险

法律合规

法律法规合规是游戏出海不可忽视的一部分。不同国家和地区对于游戏行业存在不同的法律法规，包括游戏上线审批、年龄分级制度、游戏虚拟货币等方面的规定。游戏开发者需要了解并遵守当地的法律法规，确保游戏的合法性和合规性。此外，还需要注意游戏中的消费者权益保护、广告宣传等方面的规定。

文化合规

文化适应性也是游戏出海中需要考虑的重要因素。不同国家和地区有不同的文化背景和审美观念，因此游戏内容和设计需要与当地的文化相符合。

游戏开发者在游戏开发之出便了解当地文化特点、与当地玩家进行交流、进行市场调研等，同时在上线前进行二次审核与确认，以来确保游戏内容符合当地文化风俗。

游戏作弊行为

据调研发现，出海游戏企业在所遭遇的游戏盗版、作弊方式中，50%为游戏破解包、克隆包，其次是超能力(包括穿墙、自动射击等)和改道具问题，分别为34%和32%。

综合来看，海外游戏作弊主要集中在游戏盗版和修改道具方面。海外游戏玩家主要是通过破解包来体验付费游戏或者修改游戏数据参数。而超能力则更为直接，通过修改游戏来获取游戏竞争优势。

东南亚属于外挂的重灾区，比如越南、印尼等。从全球游戏外挂特色来看，国内和东南亚地区的外挂更注重商业化，主要满足用户需求，比如实现快速击杀、自动化操作等功能；欧美地区的外挂表现为乐趣性、恶搞性质，比如在游戏中插入第三方元素等等，注重体现外挂作者自己对游戏的突破。

2024年游戏安全风险趋势

AI 对抗将在成为游戏外挂对抗常态

2023年8月11日，鹰潭市公安局余江分局网安大队接到群众余某报警，称其游戏账号被盗，许多天都登录不上，该账号他经营了几年，陆续充值了10余万元用于购买装备。

办案民警经调查发现，该团伙贩卖的“外挂”利用时下流行的智能AI算法，通过收集游戏人物的动作、表情、走位，配合自制的“DMA硬件挂”等，就能模拟玩家真实操作，无需接触游戏内部数据就可作弊，有着更强的隐蔽性。一旦发现被游戏运营团队监测、封禁，该团伙立即对产品进行迭代更新，制作新的“外挂”。

由此可见，AI已经成为外挂对抗游戏治理的一种全新的方式，而在AI加持下的外挂治理将更难。

隐藏是游戏对抗中永恒的主题

随着游戏厂商与游戏黑产的对抗的深入，黑产利用不对称的高权限使用各种方式隐藏或者伪装成正常的文件特征对抗通用的检查；使用各类加密、混淆、VMP等手段增加自身安全，提高安全人员分析的门槛；偏向辅助类，减少外挂使用者对游戏数据的暴力修改，加大的甄别的难度等。

例如，在移动端，一种名为“启动器”的外挂应用。表面上，“启动器”看似一个普通的应用，本身并不具备任何外挂或作弊功能。然而，在运行“启动器”后，它会提权，并释放真正的作弊文件到系统目录中。一旦作弊文件被释放，“启动器”应用可被卸载以避免留下任何痕迹。接着，作弊者通过本地端口使用浏览器来开启和配置这些隐藏的外挂功能。由于这些作弊文件通常不会在设备的常规应用列表中显示，这种方式极大地隐蔽了其作弊行为，有效地规避了游戏及安全服务商的传统特征检测机制。这种难以察觉的作弊手段对于游戏开发者和风控系统来说是个巨大的挑战，因为它不仅隐蔽性强，而且传统的安全措施很难对其进行有效监控和防范。

2024年游戏安全风险趋势

未成年人保护将更加严格

伴随着2024年1月1日《未成年人网络保护条例》的实施，对游戏方围绕未成年人治理的挑战将更加严峻，如何做好未成年人游戏在线时长识别与治理，游戏社区互动治理，游戏虚拟币充值治理将成为游戏公司去探索和实践的首要任务。

当然，即使《未成年人网络保护条例》没有实施，未成年人保护对于游戏公司来说也非常地重要和严峻，而伴随着立法的出台，游戏未成年人治理将向法治转变。

开放世界游戏UGC内容需要引起重视

随着开放世界游戏的兴起，游戏玩家自主创意的游戏场景将越来越多，而由此带来的游戏安全风险则走向失控。

由于开放世界游戏的自由度和开放性，一些游戏玩家在游戏中利用游戏提供的各种组件进行组合，从而搭建出不合法、不合规、破坏社会风气的建筑物。此外，AIGC在游戏内的引入，部分玩家引导智能NPC在对话中发表不当言论，从而导致玩家游戏体验环境质量下降。

对于开放世界中玩家能够自行产出、引导平台产出的内容，游戏平台需要重视起来。

跨端作弊逐年增多

在移动端，作弊者常常利用模拟器或云手机来运行游戏，同时在PC环境中使用外挂工具，这些工具通过跨平台技术读取和修改游戏内存，或者采用图像识别技术来自动化作弊行为。在PC端，作弊者可能会使用两台设备进行协同作弊：A设备用于读取游戏内存数据，而B设备则基于这些数据执行作弊操作，如通过对特定对象进行染色或进行骨骼绘制来实现透视功能，使得作弊者能够看到本不该看到的游戏内信息。这类作弊手段不仅难以检测，同时也严重破坏了游戏的公平性和玩家的游戏体验。

附件

附件：不同游戏安全风险问题与治理

如需不同游戏类型风险详情与治理实践，扫描二维码。