FairGuard
游戏加固与反外挂

FairGuard游戏安全
2023年度报告

目录

前言

据中国音数协游戏工委发布的产业报告显示，2023 年，国内游戏市场实际销售收入 3029.64 亿元，同比增长 13.95%，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。

随着疫情期间诸多负面因素明显消退，2023 年游戏行业明显回暖，用户消费意愿和能力有所回升；游戏新品集中面市并有爆款出现，与长线运营产品共同撑起收入增长；多端并发的方式，对游戏收入增长产生明显助益。

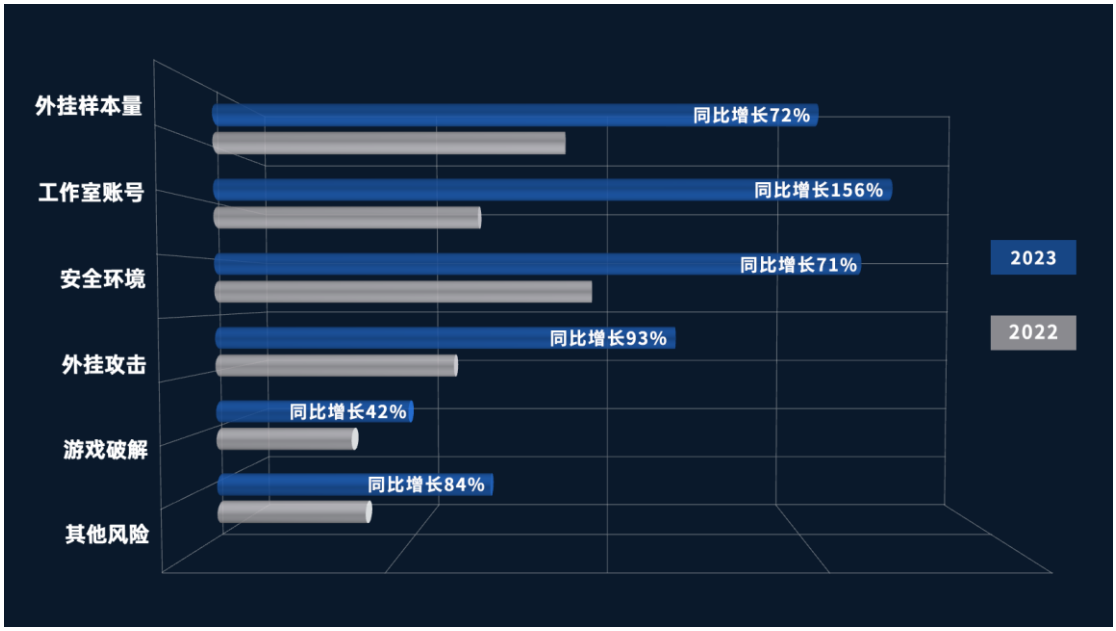
光鲜的数字背后，阴影也随之而至。整体市场表现再创新高的同时，游戏与黑灰产的对抗强度也更加激烈，各类角度刁钻的外挂、破解攻击手段层出不穷，黑产工作室技术更迭频率加快，不少游戏厂商都受到了严重的冲击，造成了不可挽回的损失。

回顾全年，游戏安全对抗更加激烈，多项数据呈上涨趋势，黑灰产呈现出技术更迭快、攻击频率高、攻击角度多样、伪装性强等特点，以下是重点内容导读：

- 安全对抗激烈，多项数据呈上涨趋势，累计检测游戏安全风险同比增长 88 % ；
- 外挂攻击方式多样，累计收集外挂样本 9976 款，同比增长 72 % ，定制注入挂约占比 78 % ；
- 游戏黑产工作室猖獗，累计封禁工作室账号 1.1 亿，同比增长 156 % ；
- 跨环境作弊对抗激烈，exe 模拟器修改外挂数量明显增多；
- 黑灰产隐匿手段更迭，运行在虚拟环境中，搭配 Magisk 工具躲避检测；
- 定制注入挂比例增加，游戏因类型与玩法不同，外挂攻击方式存在明显差异；
- 多端互通趋势下，iOS 端越狱、修改等作弊问题形式严峻。

游戏安全现状分析

01 全年游戏安全数据



▲ 2023 年 FairGuard 游戏安全数据增长对比图

据 FairGuard 游戏安全数据统计，2023 年游戏安全问题依旧严峻，游戏安全对抗激烈程度显著增加，多项数据呈上涨趋势。

全年累计检测到游戏安全风险同比增长 88 % ；

累计收集 9976 款外挂样本，同比增长 72 % ；

累计封禁的黑产工作室账号达 1.1 亿，同比增长 156 % ；

累计检测游戏环境威胁同比增长 71 % ；

累计检测游戏外挂攻击次数同比增长 93 % ；

累计检测游戏破解威胁同比增长 42 % ；

累计检测其他游戏安全威胁同比增长 84 % 。

02 游戏安全风险分布

据 FairGuard 游戏安全统计的数据分析发现，2023 年游戏黑灰产攻击角度更加多样化。主要体现在以下几方面：**工作室**（约占所有安全风险的 24 %）、**定制注入挂**（约占所有安全风险的 19 %）、**模拟点击**（约占所有安全风险的 18 %）、**内存修改器**（约占所有安全风险的 13 %）、**破解版**（约占所有安全风险的 13 %）等方面安全对抗强度明显提升。

其他常见类游戏安全风险，如：**加速器**（约占所有安全风险的 7 %）、**资源篡改**（约占所有安全风险的 3 %）、**其他游戏安全风险**（约占所有安全风险的 3 %）等方面也不容忽视。

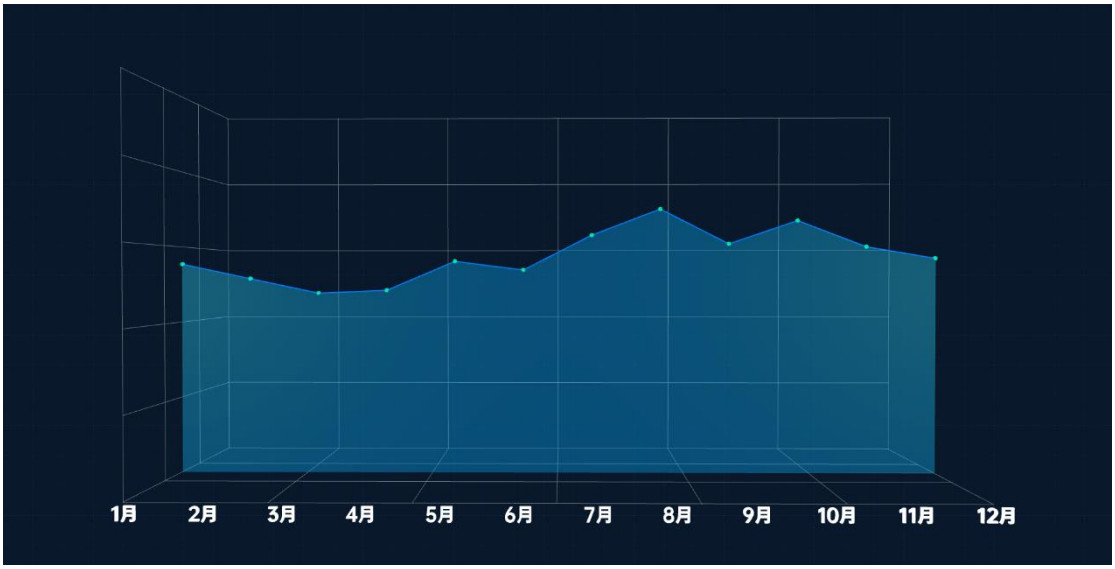
▲ 游戏安全风险分布占比图

03 游戏安全对抗时间分布

据 FairGuard 游戏安全统计的数据监测发现，游戏安全对抗强度存在较为明显的时间分布特点。

寒暑假期间与**国庆节期间**，拦截到的游戏安全风险数量会有明显攀升，说明在节

假日期间，游戏安全对抗程度相较平时会更为激烈。



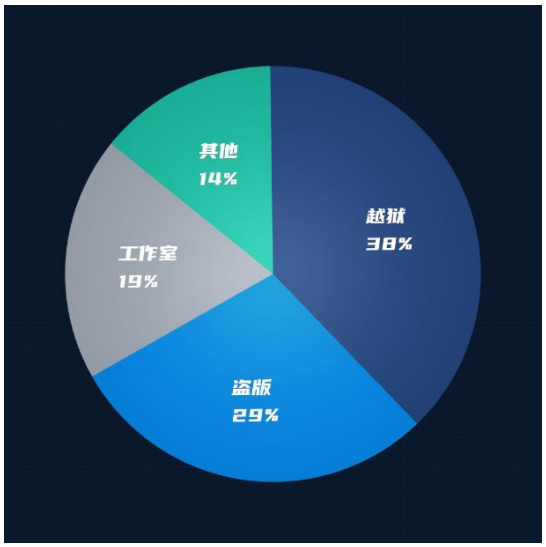
▲ 游戏安全对抗强度时间分布图

04 安卓与 iOS 外挂差异

据 FairGuard 游戏安全统计的数据分析发现，不同操作系统下，游戏黑灰产的攻击方式存在明显差异，具体表现如下：

在安卓端，游戏面临的主要安全风险为：**注入、修改器、模拟点击**。而在 iOS 端，游戏面临的主要安全风险为：**越狱环境、盗版、工作室**。

▲ 安卓端常见外挂占比



▲ iOS 端常见外挂占比

05 各类型游戏受攻击占比

据 FairGuard 游戏安全数据分析发现，因游戏品类、玩法、内容不同，游戏遭受游戏黑产攻击的情况存在明显差异。

射击类、角色扮演类、策略类游戏因品类热度高、作弊收益高、游戏数据储存在本地等因素，更容易遭受到游戏黑灰产攻击，这三类游戏受黑产攻击约占比 75% 。

值得一提的是，休闲类游戏受黑产攻击占比相较往年呈增长趋势，其他品类游戏受攻击占比相比相对较少，但游戏安全问题仍不容忽视。

▲ 各类型游戏受攻击占比图

各类型游戏安全风险分析

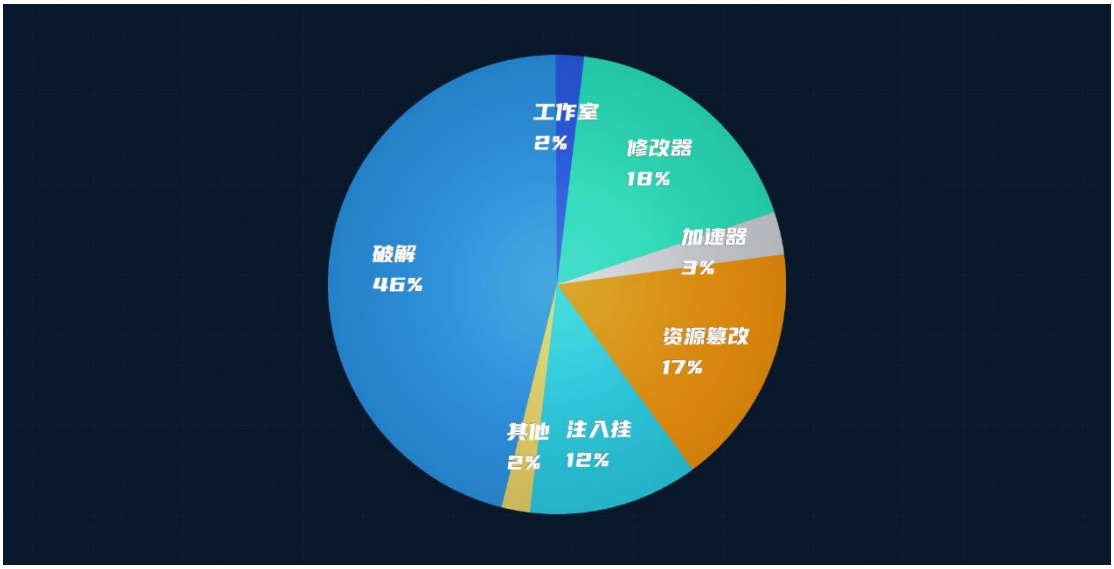
01 射击类游戏安全风险分析

射击类游戏因品类热度高、作弊收益大和数值运算储存在客户端的品类缺陷，一直以来都是游戏黑产攻击的重灾区。

据 FairGuard 游戏安全数据分析，目前射击类游戏面临的游戏安全风险主要为：**破解版**（约占所有安全风险的 46 %）、**内存修改器**（约占所有安全风险的 18 %）、**资源篡改**（约占所有安全风险的 17 %）。

由于针对射击类游戏的反外挂策略愈发完善，基于注入、修改等攻击手段的外挂数量相较往年有大幅度下降，外挂作者会采用更加刁钻的角度来破解游戏，尝试获得更高的权限，从而进行作弊来绕过检测。

此外，还有篡改关键资源文件、着色器等手段，来实现射击类游戏里的透视、穿墙等变态效果外挂，严重破坏游戏的平衡性。



▲ 射击类游戏安全风险占比图

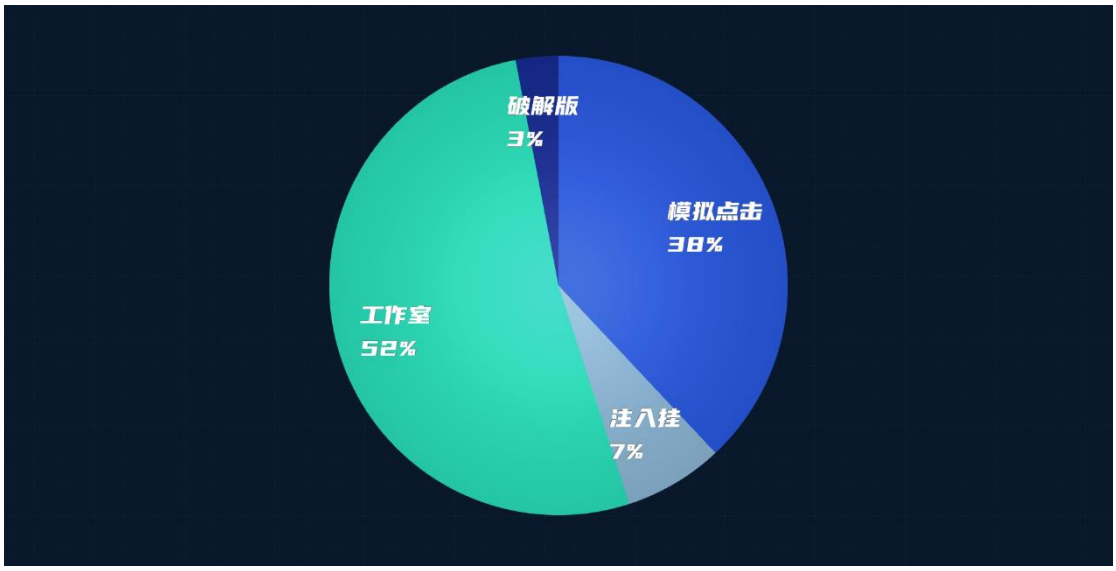
02 角色扮演类游戏安全风险分析

据 FairGuard 游戏安全数据分析，角色扮演类游戏面临的游戏安全风险主要为**脚本工作室**（约占所有安全风险的 52 % ）、**模拟点击挂**（约占所有安全风险的 38 % ）、**定制注入挂**（约占所有安全风险的 7 % ）。

近年来黑产工作室技术手段也在不断更迭，由多开群控转变为单开群控模式，采用虚拟空间、虚拟机、云手机等。

工作室可在短时间内进行大规模快速部署，搭配私有化的模拟点击脚本实现批量起号、自动跑任务、自动领取奖励，甚至部分外挂样本还存在自动战斗功能。

此外，FairGuard 收集的样本中，发现部分定制注入挂，通过注入手段，修改游戏内存模块，实现修改战斗相关数值、任务奖励、核心道具数量等功能。



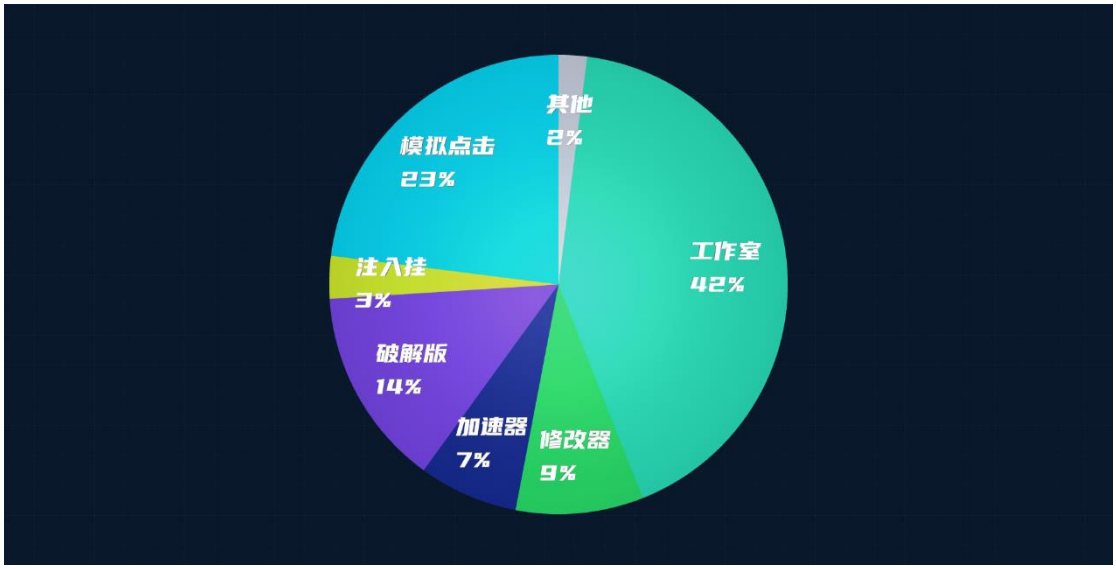
▲ 角色扮演类游戏安全风险占比图

03 策略类游戏安全风险分析

据 FairGuard 游戏安全数据分析，策略类游戏面临的游戏安全风险主要为：**脚本工作室**（约占所有安全风险的 42 %）、**模拟点击挂**（约占所有安全风险的 23 %）、**破解**（约占所有安全风险的 14 %）。

出于游戏品类及玩法特性，需要玩家保持长时间在线采集资源来获取战力，导致脚本工作室、模拟点击挂泛滥，附带的批量起号、资源售卖、自动采集、自动任务、自动战斗等外挂功能会严重破坏游戏的平衡性。

除了脚本工作室、模拟点击挂之外，部分游戏出现了通讯协议被破解的案例，游戏通讯协议破解后，客户端与服务端交互的数据会被拦截篡改，可实现修改胜负逻辑刷取资源、修改关键道具数量等功能，会破坏游戏内的公平性，导致正常付费玩家不满，值得重点关注。



▲ 策略类游戏安全风险占比图

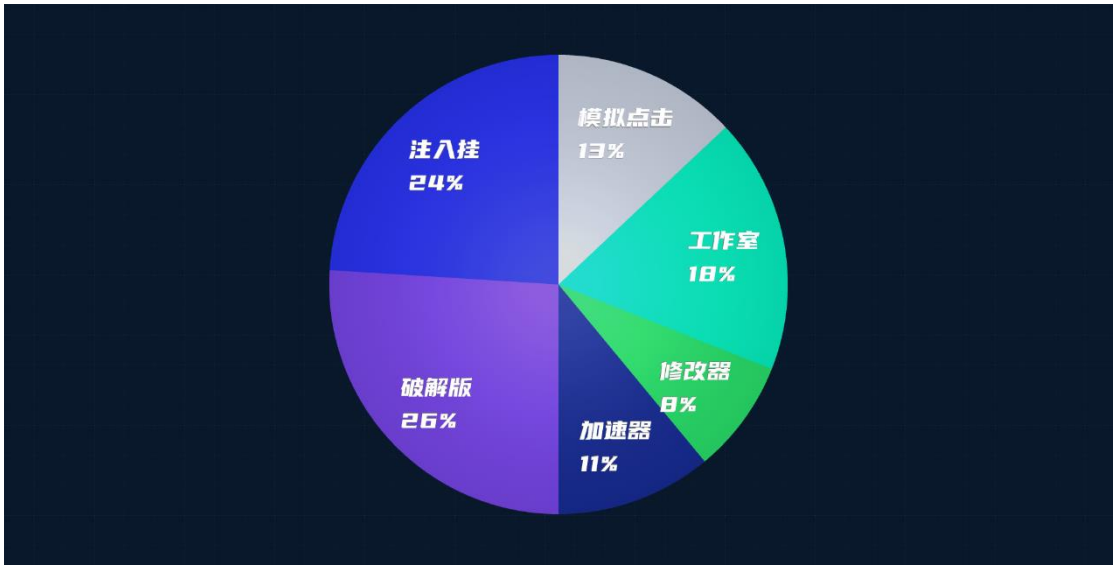
04 放置类游戏安全风险分析

据 FairGuard 游戏安全数据分析，放置类游戏面临的游戏安全风险主要为：**破解版**（约占所有安全风险的 26 %）、**定制注入挂**（约占所有安全风险的 24 %）、**工作室**（约占所有安全风险的 18 %）与**模拟点击**（约占所有安全风险的 16 %）。

外挂作者可通过注入或修改器来篡改游戏内的数值模块，可以修改游戏内金币/钻石来实现无消耗、快速养成，会对游戏公平性造成极大影响。

此外，放置类游戏玩法需要玩家定期点击收集道具，所以模拟点击挂问题比较常见。

放置类游戏还面临严重的破解问题，游戏被破解产生的的盗版、内购破解版、无广告版等，会导致正版玩家大量流失，严重缩短游戏生命周期。



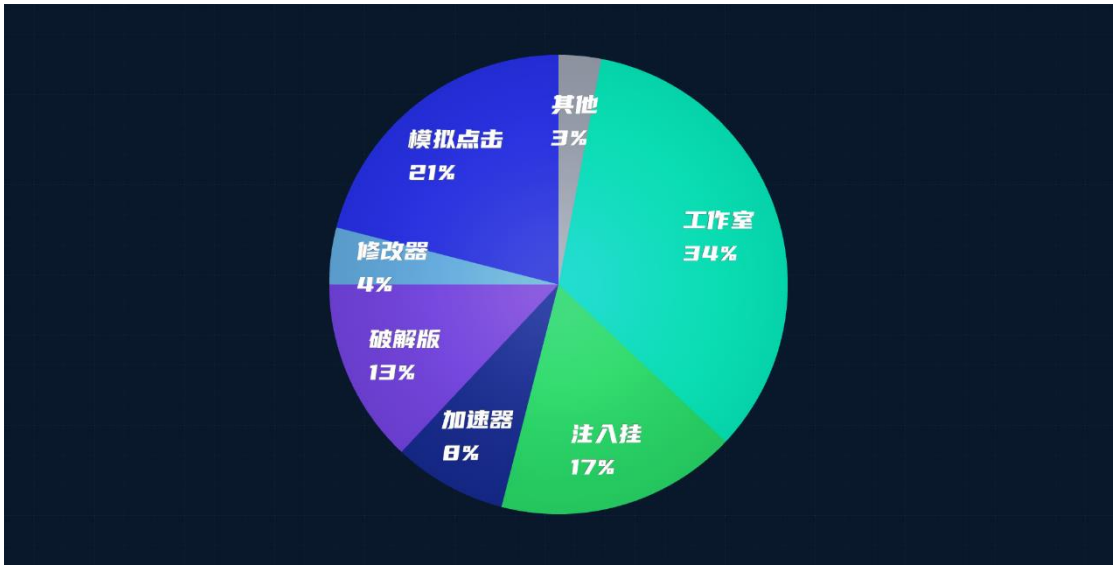
▲ 放置类游戏安全风险占比图

05 卡牌类游戏安全风险分析

据 FairGuard 游戏安全数据分析，卡牌类游戏面临的游戏安全风险主要为：**脚本工作室**（约占所有安全风险的 34 %）、**模拟点击挂**（约占所有安全风险的 21 %）、**注入挂**（约占所有安全风险的 17 %）。

卡牌类游戏往往会面临大量的脚本工作室，搭配使用模拟点击脚本，实现批量起号、刷金币号及初始号的问题。

其次较多的是注入、破解问题，如通过修改卡牌数据来获取不平等对抗优势；通过破解通讯协议，来实现篡改游戏抽卡数据等作弊手段，值得重点关注。



▲ 卡牌类游戏安全风险占比图

06 休闲游戏安全风险分析

据 FairGuard 游戏安全数据分析，休闲类游戏面临的游戏安全风险主要为：**破解**（约占所有安全风险的 44 %）、**内存修改器**（约占所有安全风险的 26 %）、**定制注入挂**（约占所有安全风险的 13 %）。

休闲类游戏是破解的重灾区，外挂作者可通过反编译手段，篡改游戏逻辑，剔除广告模块，加入恶意功能模块，制作出游戏破解版、无广告版，会对正版游戏产生巨大冲击。

休闲类游戏还面临着注入、修改器等篡改游戏内数值，获取相关道具跳过广告的案例，此外，游戏存档提取售卖问题也同样值得关注。

▲ 休闲类游戏安全风险占比图

FairGuard 游戏安全部分热门功能简介	
防护功能	**功能描述**
游戏引擎加密	FairGuard 独家无导入函数 SO 加壳技术，深入游戏底层提供最强级别加密防护，保护游戏代码不被分析，防止破解者的进一步操作。
资源加密	FairGuard 独家资源加密方案，深入游戏引擎底层，结合游戏资源文件结构及加载机理精心构造，可为游戏提供高强度加密保护，具备运行消耗小、性能无影响的特点，支持 Android/iOS/PC 三平台。
防破解	FairGuard 业界独家无 API 签名校验技术，对游戏的引擎与代码进行深度加密，并对游戏包签名和文件完整性进行多重校验，防止游戏被植入恶意模块、剔除广告等。
反外挂	针对游戏将面临一系列外挂修改风险，FairGuard 研发了行为检测方案，搭配 200+维度的智能感知系统，可通杀各类外挂及其变种，做到有效防护。
反注入器	禁止使用 Xposed、Frida 等各种外挂模块注入器，防止注入后修改游戏内存等各种恶意行为，一旦发现立即闪退。
反调试	防止外挂作者对游戏进行调试，阻止对游戏的静态或动态分析，一旦发现立即闪退。
反引擎级变速	深入游戏引擎底层，对引擎级的变速进行深度检测，获取具体变速倍数，可实现精准封号打击或闪退处理。

变速无效化	采用 FairGuard 独家无导入函数 SO 加壳技术，高强度加壳保护游戏内代码，经大量实机测试，可无视任何变速器及其变种，使其变速功能无效化。
安全环境检测	采用底层检测手段，精准识别游戏运行环境，如：越狱、ROOT、虚拟机、虚拟框架、云手机等，并提供个性化闪退策略。
主动识别恶意模块机制	FairGuard 独家方案，无需获取注入挂样本，可对游戏内可疑模块进行主动识别，搭配在线打击功能做到主动防御，大幅缩短外挂排查周期。
数据校验	精准校验游戏上下行数据，最大程度上保证游戏通讯协议安全。
支付保护	可对游戏支付过程进行保护和校验，防止篡改支付过程绕过付费或替换收款帐号掠夺玩家付费的现象发生。
态势感知	FairGuard 独家方案，可对无特征的私有脚本进行智能分析挖掘，定位并标记出工作室账号，可自动对接给游戏方进行封号处理，做到高效防护。

如您有其他游戏安全问题

欢迎添加微信咨询

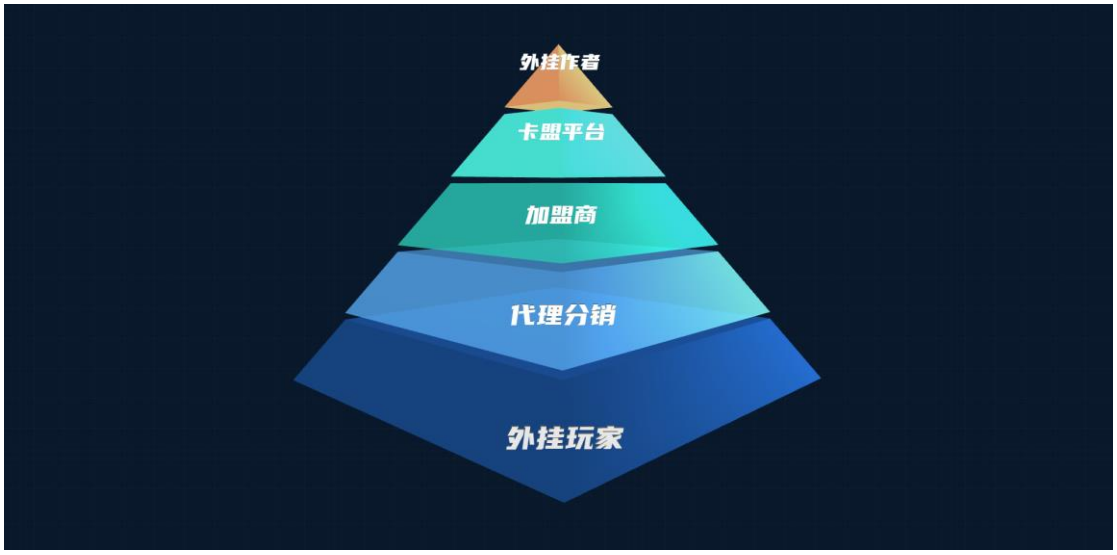
单元安全问题分析

01 黑灰产业链

据 FairGuard 观察分析，近年来游戏黑灰产的攻击角度愈发多样，会根据游戏的玩法与内容，同时出现多种情况，如：游戏外挂、游戏破解、资源解包、搭建私服、资源工作室等。

这些行为会对游戏厂商的收益造成直接影响，并破坏游戏的公平性和正常付费玩家体验，严重的情况甚至会缩短游戏生命周期。

据观察，当下游戏黑灰产业链发展已十分成熟，以外挂制售为例，产业链由外挂作者、卡盟平台、加盟商、代理分销组成，呈金字塔形状分布。



▲ 游戏外挂制售黑灰产业链

黑灰产上游为外挂作者，专职开发各类外挂软件，钻研游戏存在的安全漏洞，具备较强的反侦查和反检测能力。

外挂作者开发外挂后，会联系卡盟平台进行发布，由加盟商与代理分销一层层向下扩散。

最终，外挂会通过 QQ 群、网购平台、游戏社区、游戏盒子、外挂平台等渠道触达开挂玩家，同时开挂玩家内部也会进行二次传播。

02 黑产工作室

黑产工作室，是指依靠特殊设备进行游戏，异常获取游戏内的金币/道具/奖励等资源，再通过交易或转移等手段将资源进行变现的组织。

据观察，当下游戏黑产工作室产业链规模庞大，涉及到非黑名单 ip 代理、伪造信息设备、身份资料等灰色产业，通过这些资源来伪装躲避检测。

随着黑产技术迭代，与工作室的对抗难度也直线上升，工作室牟利手段由多开群控转变为单开群控模式，多采用虚拟空间、虚拟机、云手机等方式，在短时间内进行大规模部署，并拥有在线部署的弹性能力，可迅速将收益转移，需要游戏安全产品具备更高的识别效率。

工作室类型	工作室牟利路径
打金工作室	通过非正常游戏手段，利用大量角色掠夺游戏资源，并转售变现，导致游戏经济系统失衡崩坏。
代练工作室	使用与该游戏玩法相关的辅助软件，完成一系列操作，如自动日常、自动采集等。
资源囤积号	利用游戏内经济系统，通过囤积、炒作等手段将游戏内资源以高价卖给正常玩家，以此牟利。
初始号、自抽号	通过脚本、脱机等非正常手段快速起号，获取游戏任务奖励，再低价售卖给玩家，严重影响营收。

▲ 常见的游戏工作室类型及牟利方式

脚本私有化更是加大了检测难度，工作室在脚本中加入社交、休息等行为，伪装成正常玩家来躲避检测，要通过游戏行为来区分工作室与正常玩家，需要游戏安全产品具备更精准的识别能力。

此外，FairGuard 收集的样本中还发现，有些工作室通过代理或 VPN 等方式伪造 IP 地址，更有甚者可**伪造设备指纹**，让一般的检测手段难以追踪，是对游戏安全产品技术力的重大考验。

游戏打金工作室掠夺游戏资源，导致物价与金币贬值的行为，会严重破坏游戏经济体系，不仅损害了官方的利益，还会造成正常付费玩家流失等现象，缩短游戏生命周期。

03 黑卡充值

黑卡充值常隐匿于“代充”服务中，且形式多变，常见的有黑卡、退款、36 漏洞、库存系统、盗刷信用卡，以及基于 bundleID 漏洞的新型内购欺诈。

“bundleID 漏洞”是黑产在其他应用上以低价（1 元）充值获取的真实支付凭证，再在游戏中购买高价商品（648 元），如果游戏服务端苹果凭证校验接口存在漏洞，只校验了凭证中商品和订单信息，未校验凭证中 bundleID，则会验证通过，进而发货，产生坏账。

“库存系统”是代充工作室与黑灰产勾结，利用越狱设备搭配插件，将电信诈骗、盗刷信用卡等方式获得的黑产，以充值购买游戏礼包的形式获得“支付成功”凭证，再将支付凭证以“代充”形式兑现，从而导致坏账。

此外，还有利用小额支付漏洞、盗刷等多种手段的黑卡代充，这类黑卡充值在各种渠道打着低价代充游戏礼包的噱头，吸引玩家购买。黑卡充值过程中，平台没有收到金额，但游戏产品却已经兑现，等到游戏厂商与平台结算时，就产生了大量的坏账，严重损害了游戏厂商的收益。

04 exe 模拟器外挂

这类外挂本质是内存修改器，原理是通过多次搜索数值对内存模块进行定位，再确认后对数值模块进行篡改，从而实现外挂效果。

通用的内存修改器检测起来并不困难，采用**安全环境检测**或**外挂行为检测手段**即可进行有效防护，而这类新型外挂，为了躲避检测，并不需要在 Root 环境下运行。

PC 跨模拟器外挂以 exe 程序运行在 PC 端，而游戏运行在 PC 模拟器中，外挂不再读写游戏程序内存，而是读写整个模拟器中的数据，通过反复定位，也可以实现内存修改的效果。

这类外挂有两大检测难点：

- 无需开启 Root 权限即可搜索内存进行数值篡改，让以往的安全环境检测方案难以排查。

- 游戏在运行过程中，数值会实时变动，进行数值排查需要耗费更久的周期，严重影响对抗效率。

04 H5 游戏安全问题

小游戏热度高、玩家体量大，也更容易被游戏黑灰产所侵扰，相较于端手游而言，小游戏的破解难度更低，也造成了市面上小游戏破解、扒包事件频发。小游戏主要面临以下几类游戏安全问题：

- 小游戏被破解、扒包

破解与扒包，是小游戏面临的主要安全风险，破解者可通过各类工具对小游戏包体进行分析、破解，获取包内的源代码及各类资源。

在保留游戏框架的基础上，对游戏包内的美术资源、广告模块进行替换，进行重打包并上架，这种行为会对原游戏方的收益造成严重影响。

- 游戏资源泄露

游戏包体被破解后，会造成包体内的代码、图片、视频、音频等资源泄露，这些资源可能会被用作竞品分析，甚至是换皮上架，对游戏会产生不可估量的损失。

- 通讯协议破解

破解者可通过抓包工具破解游戏通讯协议，破坏正常的游戏客户端与服务端交互流程，从而实现篡改数据、游戏内逻辑等行为，这种行为会导致正常玩家不满，对厂商口碑、收益造成影响。

其他安全问题分析

01 隐私合规

自 2021 年以来，国家陆续出台了《个人信息保护法》、《网络安全法》、《APP 违法违规收集使用个人信息行为认定方法》等律法，建立了相对健全的隐私保护制度。

工信部也曾多次开展关于 APP 侵害用户权益专项整治行动，对“APP、SDK 违规处理用户个人信息”“设置障碍、频繁骚扰用户”“欺骗误导用户”等问题进行严格排查。

各大应用商店建立了严格的 APP 上架审核机制，在上架和更新过程中，均进行严格监督，来确保应用没有存在违规获取隐私权限等行为。如果应用存在违规获取隐私现象，会导致上架审核不通过或应用下线整改等严重后果。

游戏出现此类问题主要原因是在支付、广告、渠道分包、数据分析等环节需要植入第三方 SDK，而第三方 SDK 常常存在不符合上架规定的权限获取行为，游戏方应当重点关注。

02 虚假用户刷量

虚假用户刷量是营销欺诈行为的一种，指工作室通过脚本模拟真实用户的行为，进行交互、安装、捏造貌似合法的虚假活动，盗取游戏的 CPI 和 CPA 营销预算。

虚假安装最初起源于“设备农场”，一种通过操控大量真实设备进行虚假安装，以达到盗取广告预算的工作室。随着技术更迭，作弊者转而利用更先进的技术注

入虚假安装，将真实设备连接到中心主机，同时运行脚本，自动伪造交互和安装进程。

在近期收集的样本中，作弊者为了进一步降低成本，放弃了真实设备，直接采用虚拟机、云手机等环境。作弊技术的更迭与自动化让虚假用户刷量所需的资源更少且收益更高，导致其更加猖獗。

为了伪造安装，作弊者会依靠服务器虚拟化和模拟软件同时模拟许多台设备。在每台设备上，作弊者会创建一个用户，然后为该用户创建脚本，使之通过点击与广告进行交互。

仿真设备会下载目标应用并将其打开，以便触发安装事件，随后该事件将被传输给归因提供商。作弊者甚至会更进一步将会话存储起来供以后使用，在之后几天再次打开应用，看起来就像是创建了另一个会话,以及一个活跃用户。

关于 FairGuard

FairGuard 是杭州法嘉德科技有限公司创立的游戏加固产品的品牌。公司专注于游戏加固及反外挂领域，致力于帮助游戏公司解决外挂和破解问题，为游戏提供深度一体化的加密保护方案。

FairGuard 开发团队深耕技术，研发了无导入函数 SO 加壳、无 API 签名校验、三端通用的 Unity Assetbundle 资源加密方案等多项业界独家技术。

公司始终坚持自主研发、客户至上的服务理念，秉承专注、极致、口碑的企业精神，通过专业的服务，为客户提供优质的游戏安全解决方案，赢得了客户的一致好评。

目前，产品已经被 FunPlus、三七互娱、游族、恺英网络、心动网络等多家头部游戏公司采用，接入 400+款热门游戏。

扫码关注微信公众号

扫码添加客服微信

7×24 小时为您服务