FairGuard
游戏加固与反外挂

FairGuard游戏安全
2022年度报告

目录

前言 01

游戏安全现状分析 02 / 04

不同游戏类型
安全风险分析 05 / 11

其他安全问题分析 12 / 14

关于FairGuard 15

前言

据中国音数协游戏工委发布的产业报告显示，2022 年中国游戏市场实际销售收入 2658.84 亿元，同比减少 306.29 亿元，下降 10.33 %；游戏用户规模 6.64 亿人，同比下降 0.33 %。

2022 年游戏行业在版号发放数量缩减、企业生产研发受限、未成年人保护政策监管趋严、宅经济的刺激效应减弱等因素影响下，多项市场指标出现下滑，行业整体处于承压蓄力阶段。

与遭遇寒冬的市场表现相反，游戏黑灰产规模在迅速壮大，外挂、破解、黑产工作室等攻击手段层出不穷，不少游戏厂商受到了严重的冲击，造成了不可挽回的损失。

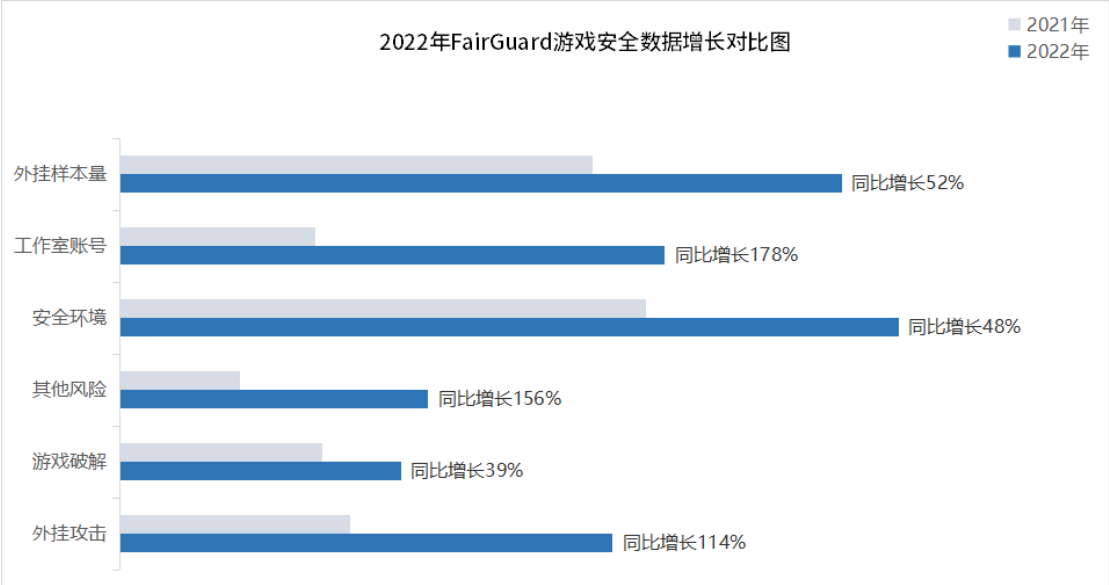
回顾全年，游戏安全对抗更加激烈，多项数据呈上涨趋势，游戏黑灰产攻击呈现出伪装性强、攻击频率高、攻击角度多样化等特点。

- 安全对抗更激烈，多项数据呈上涨趋势，累计检测游戏安全风险同比增长 96%
- 游戏外挂攻击方式多样化，累计收集外挂样本 5826 款，同比增长 52 %
- 游戏黑产工作室猖獗，累计封禁工作室账号 4378 万，同比增长 178 %
- 高维作弊对抗激烈，手游 PC 跨模拟器外挂数量明显增多
- 黑灰产攻击呈现出攻击频率高、攻击角度多、伪装性强等特点
- 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

游戏安全现状分析

01 全年游戏安全数据

据 FairGuard 游戏安全数据统计，2022 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 96 % ；

累计检测游戏外挂攻击次数同比增长 114 % ；

累计检测游戏破解威胁同比增长 39 % ；

累计检测其他游戏安全威胁同比增长 156 % ；

累计检测游戏环境威胁同比增长 48 % ；

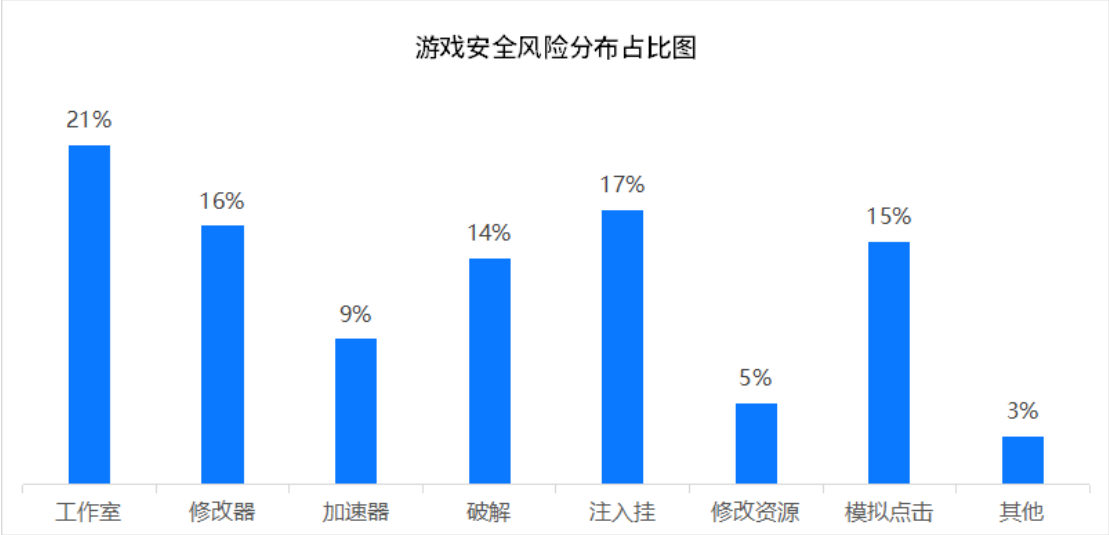
累计封禁的黑产工作室账号达 4378 万，同比增长 178 % ；

累计收集 5826 款外挂样本，同比增长 52 %。

02 游戏安全风险分布

据 FairGuard 游戏安全统计的数据分析发现，2022 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 21 %）、定制注入挂（约占所有安全风险的 17 %）、内存修改器（约占所有安全风险的 16 %）、模拟点击（约占所有安全风险的 15 %）、破解（约占所有安全风险的 14 %）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 9 %）、资源篡改（约占所有安全风险的 5 %）、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。



03 游戏安全对抗时间分布

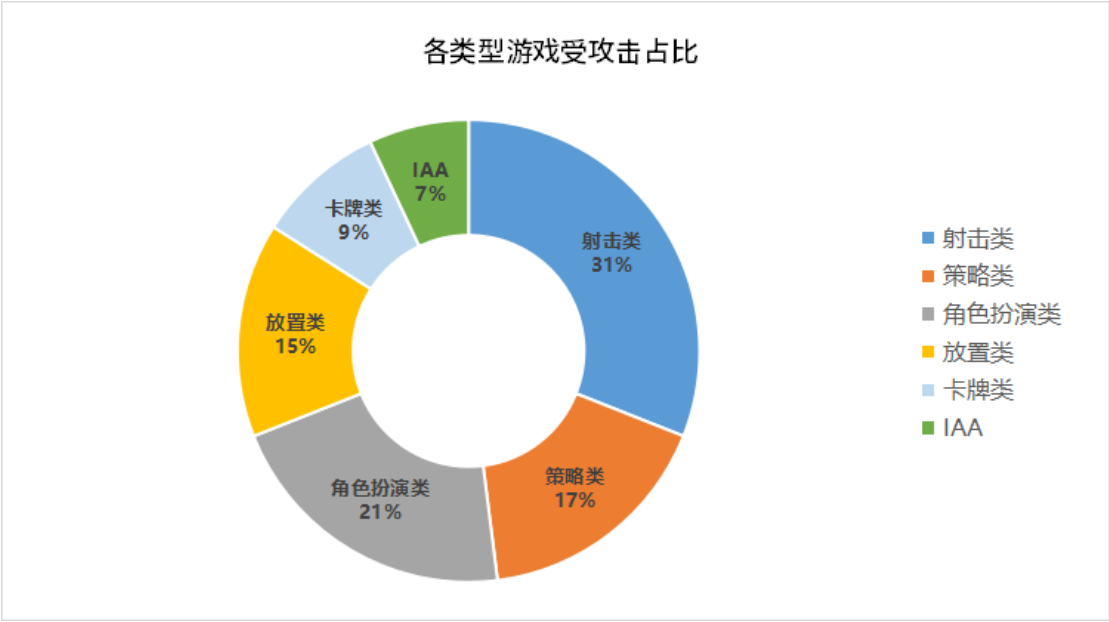
据 FairGuard 游戏安全统计的数据监测发现，游戏安全对抗强度存在明显的时间分布的特点。

寒暑假与国庆节期间，拦截到的游戏安全风险数量会有明显攀升，说明期间游戏安全对抗程度会更为激烈。

04 各类型游戏受攻击占比

据 FairGuard 游戏安全数据分析发现，不同品类游戏遭受游戏黑产攻击的占比不同。

射击类、角色扮演类、策略类游戏因品类热度更容易受到游戏黑产攻击，合计占比近 7 成。其他品类游戏受攻击占比相比较少，但游戏安全问题仍不容忽视。



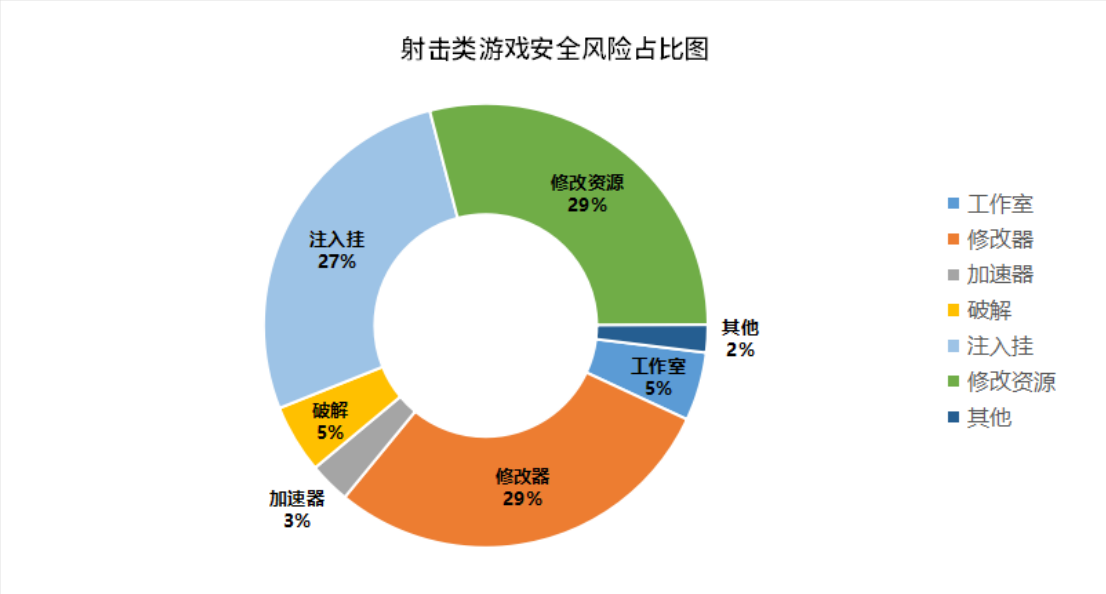
不同游戏类型安全风险分析

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，射击类游戏面临的游戏安全风险主要为：修改资源（约占所有安全风险的 29 %）、内存修改器（约占所有安全风险的 29 %）、定制注入挂（约占所有安全风险的 27 %）。

外挂作者可通过多种角度，修改内存模块、篡改关键资源文件，来实现射击类游戏里常见的锁血、加速、瞬移、锁头、飞天、透视、穿墙等变态效果外挂，严重破坏游戏的平衡性。

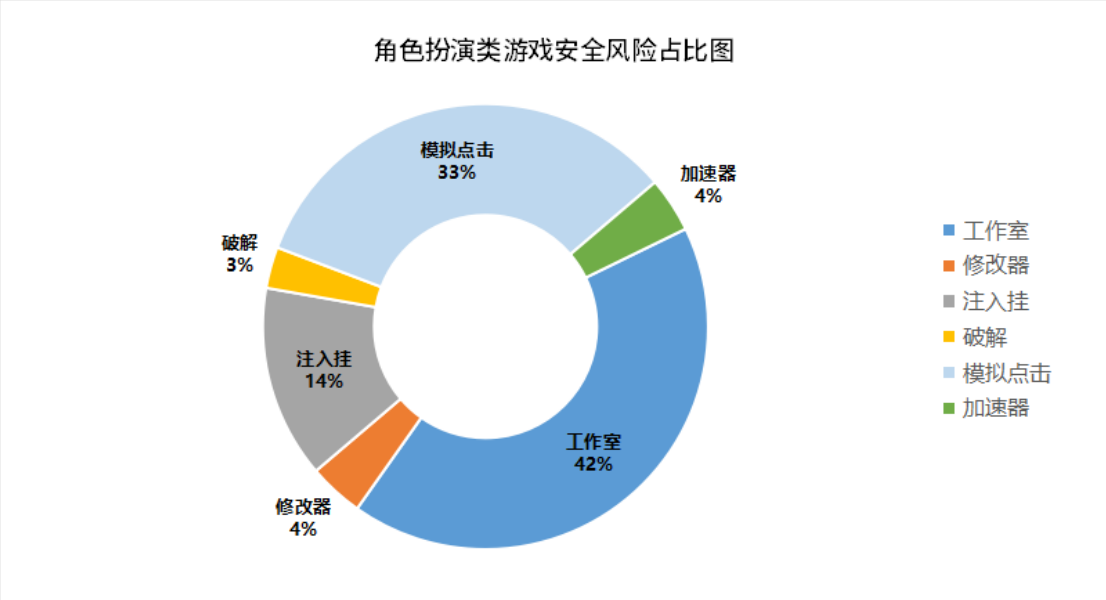


02 角色扮演类游戏安全风险分析

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 42 %)、模拟点击挂(约占所有安全风险的 33 %)、定制注入挂（约占所有安全风险的 14 %）。

工作室采用多开群控或云手机等方式可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，实现修改修改战斗相关数值、任务奖励、核心道具数量等功能。

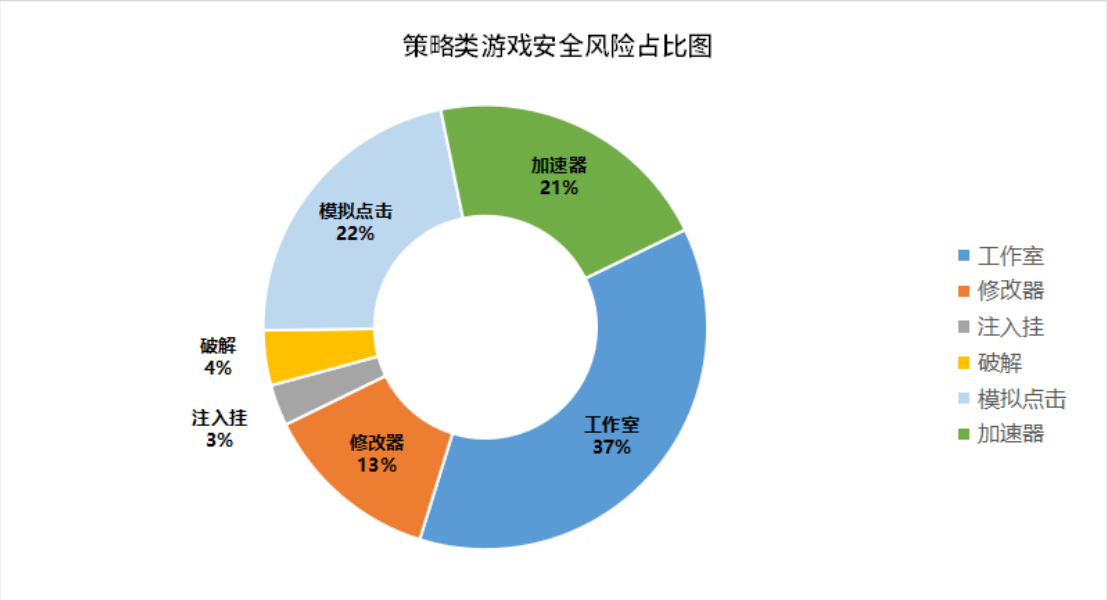


03 策略类游戏安全风险分析

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 37 %）、模拟点击挂（约占所有安全风险的 22 %）、加速器（约占所有安全风险的 21 %）。

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，还有大量通过加速器来实现快速获取游戏资源，缩短养成周期的案例也值得重点关注。

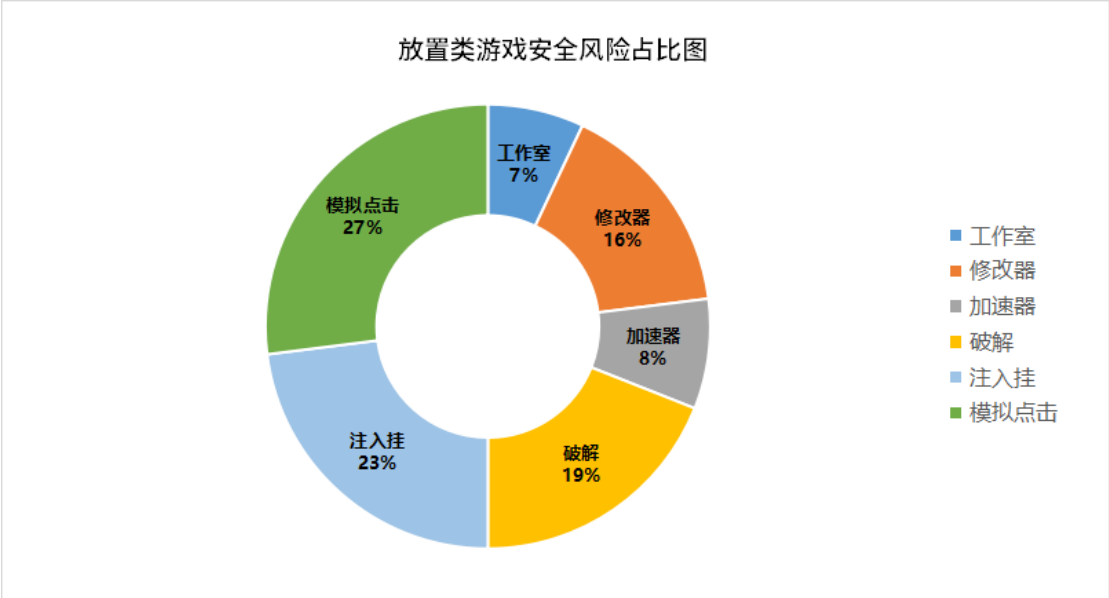


04 放置类游戏安全风险分析

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：模拟点击挂（约占所有安全风险的 27 %）、定制注入挂（约占所有安全风险的 23 %）、破解（约占所有安全风险的 19 %）与内存修改器（约占所有安全风险的 16 %）。

由于放置类游戏玩法需要玩家定期点击收集道具，所以模拟点击挂最为常见。此外，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。

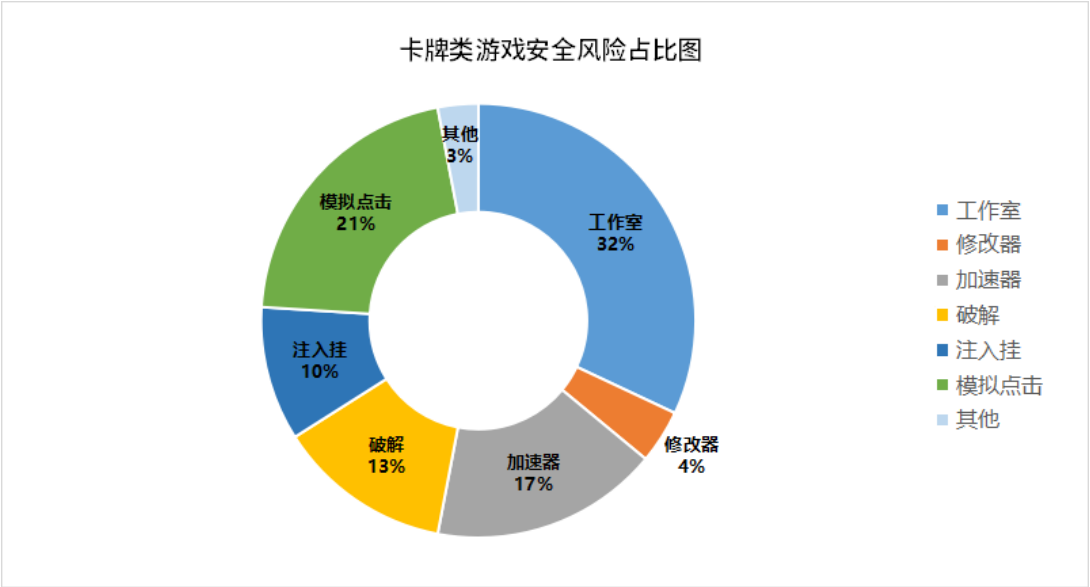
放置类游戏还经常面临破解问题，游戏的盗版、内购破解版、无广告版等内容，会严重缩短游戏生命周期。



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 32 %）、模拟点击挂（约占所有安全风险的 21 %）、加速器（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进行批量起号，刷金币号、初始号的问题。其次较多的是加速器问题，如延长己方出牌环节时间、加速己方出牌环节动画，从而进行作弊。

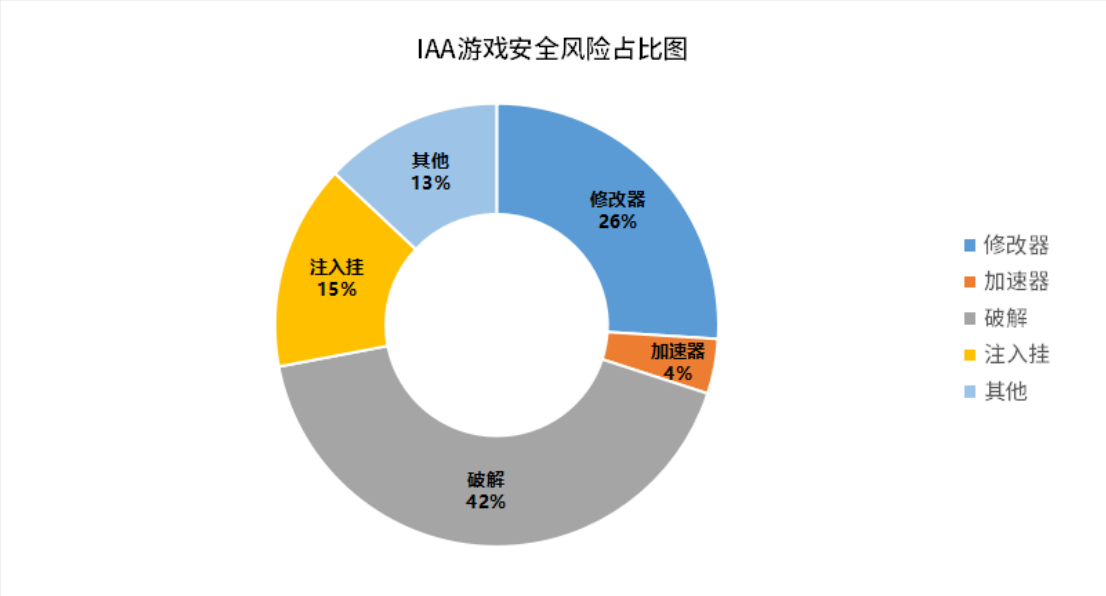


06 IAA 游戏安全风险分析

据 FairGuard 游戏安全数据分析，IAA 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 42 %）、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 15 %）。

IAA 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。

IAA 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。



FairGuard 游戏安全部分热门功能简介	
防护功能	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。
防破解功能	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。
反外挂功能	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。
反注入器功能	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。
反调试功能	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。
数据校验功能	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。
支付保护功能	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。
态势感知功能	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

其他安全问题分析

01 打金工作室

所谓「打金工作室」，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，其行为会对游戏的经济系统造成严重影响，损害游戏厂商的利益。

随着黑产规模壮大，技术迭代，与打金工作室的对抗难度也直线上升。工作室采用多开群控或云手机等方式可进行大规模快速部署，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。

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。

02 黑卡充值

黑卡充值常隐匿于「代充」服务中，且形式多变，常见的形式有外币汇率差、退款、36 漏洞、黑卡、盗刷信用卡，甚至还出现了专门的库存系统。

「36 漏洞」是利用 iOS 小额支付漏洞实现的刷单套利业务。苹果为提高用户体验，在 APP Store 购买商品时，对小额支付不进行验证，当用户发起 6 元、30 元金额的消费订单时，苹果会直接向游戏运营商发送“支付成功”凭证。

而「库存系统」，则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，再将凭证进行拦截并纳入库存系统。

代充工作室在各种渠道打着低价代充游戏礼包的噱头，吸引玩家购买，在支付过程将库存中的成功凭证兑换成游戏礼包。

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。

03 隐私合规

工信部曾多次开展关于 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。

04 PC 跨模拟器外挂

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。

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、BiliBili、Garena、心动网络等多家头部游戏公司采用，接入 200+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