Anti-Cheat Expert | 腾讯云

2021 游戏安全白皮书

GAME SECURITY WHITE PAPER

2021

目录
CONTENTS

01/02
引言
INTRODUCTION

03/10
外挂问题
CHEATING PROBLEMS

11/14
打金工作室和游戏黑产资产
GAME BOTS AND BLACK MARKET ASSETS

15/17
信息安全问题
INFORMATION SECURITY PROBLEMS

18/21
游戏云上安全问题
GAME SOFTWARE PIRACY PROBLEMS

22
游戏盗版问题
GAME SOFTWARE PIRACY PROBLEMS

23/28
其他游戏安全问题
OTHER GAME SECURITY PROBLEMS

29/30
关于ANTI-CHEAT EXPERT
ABOUT ANTI-CHEAT EXPERT

引言
INTRODUCTION

据《2020年中国游戏产业报告》显示，2020年，中国游戏产业收入达2786亿元，同比增长20.71%。而据《2021年1-6月中国游戏产业报告》显示，2021上半年，中国游戏用户达到6.67亿，同比增长1.38%；游戏市场实际销售收入1504.93亿元，同比增长7.89%。游戏行业强劲的发展势头，正吸引着越来越多的游戏厂商入局，产业快速发展的同时，游戏黑产的获利手段也在不断演变，给不少游戏带来了严重的冲击。

据腾讯游戏安全统计数据，2020年，腾讯协助警方办理游戏安全相关案件数达13起，抓捕犯罪嫌疑人120人。游戏黑产涉足的范围甚广，包括外挂、打金工作室、恶意刷奖励、信息安全、DDoS攻击、游戏代练、游戏“演员”等。

01/2021年游戏安全问题依旧严峻

2020年-2021年上半年，腾讯游戏安全检测到的游戏黑产帐号数超过1亿，其中游戏打金工作室帐号量超过6680万个

2020年-2021年上半年，游戏外挂样本数达49000款以上，其中移动游戏外挂在2020年呈现爆发式增长，同比去年增长了118%

2020年全年游戏内的违规文本信息超过300亿条

02/调研

腾讯游戏安全近期一项覆盖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两大原因之一，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，全部被访游戏厂商均表示有自建的安全技术对抗团队或使用过外部相关的游戏安全产品。

由此可见，无论是对于玩家或者游戏厂商，游戏安全问题都已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。

不同的游戏品类，其主要面临的安全问题的也有所不同，具体如下图所示:

	动作射击类游戏（STG）	多人在线竞技类游戏（MOBA）	角色扮演类游戏（MMORPG）	策略类游戏（SLG）	休闲类游戏
外挂	★★★★★	★★★★★	★★★★	★★★	★★★★★
打金工作室和黑产	★	☆	★★★★★	★★★★	★★
违规内容信息	★★★	★★★★★	★★★	★★	★★★★
消极游戏行为	★	★★★★	☆	☆	☆
演员	☆	★★	☆	☆	☆
代练	☆	★★★	★	☆	☆
帐号安全	★★★★	★★★★	★★★★★	★★★	★★★
盗版	★★★	★★★	★★★	★★★	★★★

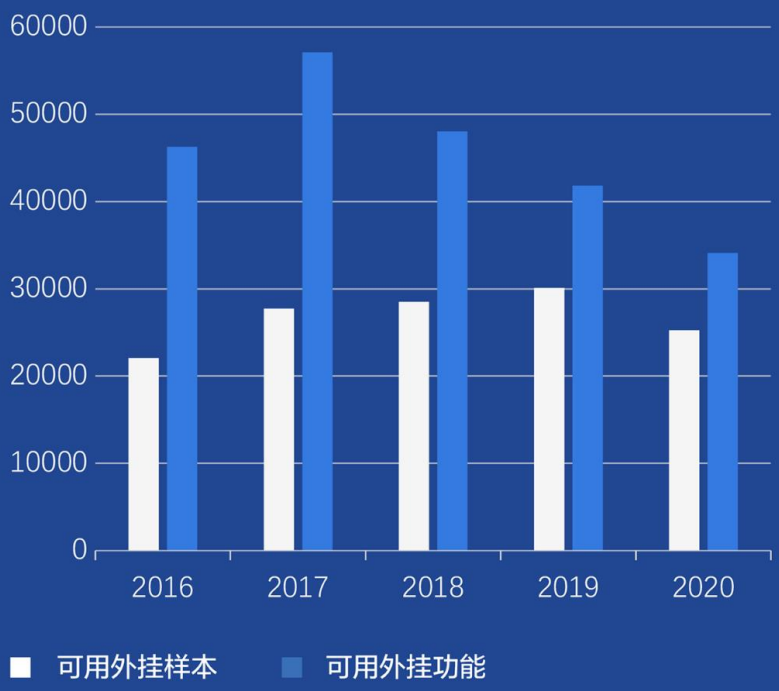
备注：★越多表示面临的挑战越大，同时，游戏日活跃量越大，上述问题的严重性更加突出

外挂问题
CHEATING PROBLEMS

01 /端游外挂问题

2020年腾讯端游外挂样本数及功能数较去年均有所下降

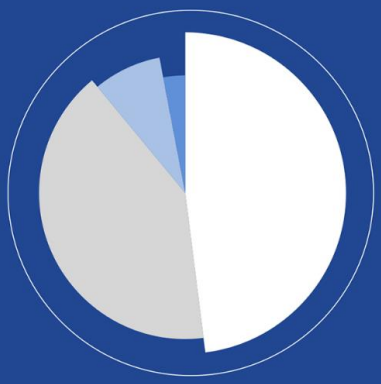
腾讯PC端游戏近年来监测到的外挂样本数及功能数



伴随PC端游戏市场规模的减少，2020年，PC端游戏的外挂样本数及功能数比2019年均有所下降，但整体外挂的绝对数量依然很高，外挂对抗仍旧激烈，2021年上半年，PC端游戏的外挂样本数达10137个。

射击类、大型多人在线角色扮演类及休闲竞技类游戏外挂问题最严重

2020年腾讯不同类型端游检测到的外挂分布图



- 48% 射击类
- 41% 大型多人在线角色扮演类
- 8% 休闲竞技类
- 3% 多人在线战术竞技

2020年，在PC端游戏外挂样本中，射击类游戏的外挂样本数占比最高，占总体PC端游外挂数的48%，其次为MMORPG游戏，占总体PC端游戏外挂数的41%。

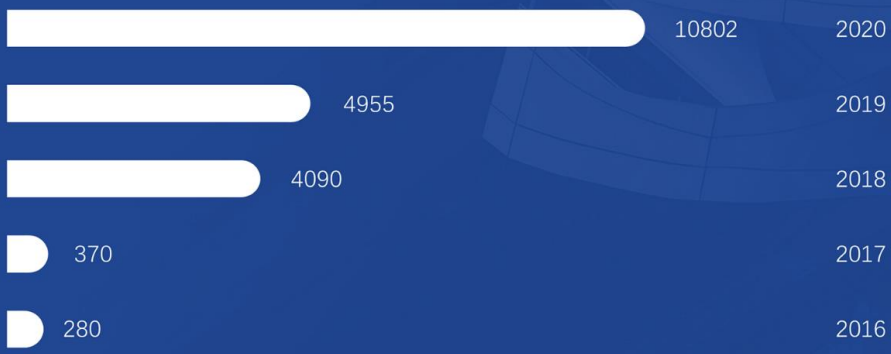
休闲竞技类、多人在线战术竞技类游戏的外挂问题也不容忽视。其中，在多人在线战术竞技类游戏中监测到的外挂样本数也占到射击类游戏的7.4%。

相比2019年，PC端游戏中的大型多人在线角色扮演类游戏的外挂占比有所下降，射击类游戏外挂占比有所上升。需要注意的是，游戏重点模式和玩法更容易吸引外挂的青睐，外挂对游戏口碑带来的影响也十分明显。

02/手游外挂问题

2020年腾讯手游监测到的外挂数比去年翻了一番

腾讯手游近年来监测到的外挂数



随着移动游戏数量的增长，移动游戏外挂样本数从2016年起，便逐年快速增长。到2020年，移动游戏外挂更是呈现爆发式增长，移动游戏外挂样本数达10802款，同比去年增长了118%，而2021年上半年，移动游戏外挂样本数为3350个，外挂功能却达到了13800个。

射击类、休闲类、多人在线竞技类游戏外挂问题最严重

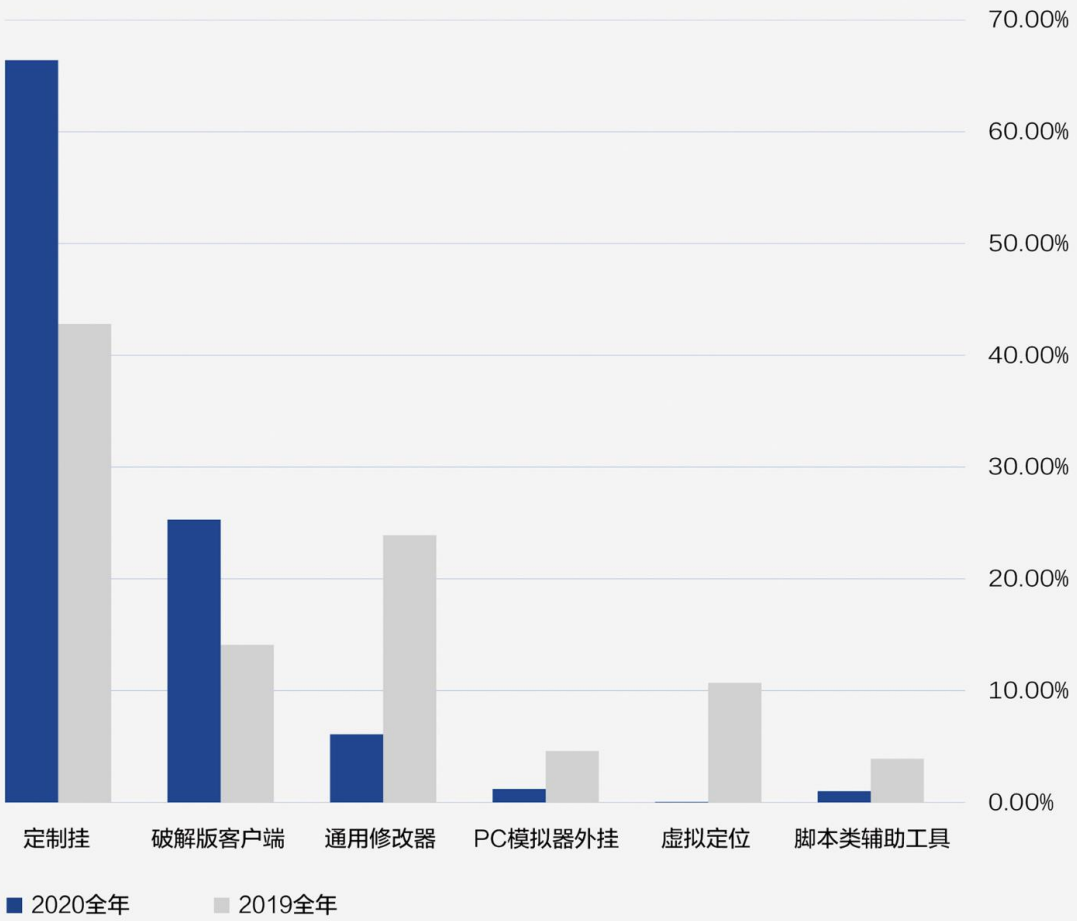
不同类型游戏的外挂处罚量占该品类游戏日活量占比（相对值）

从不同品类游戏的外挂处罚量与日活跃占比相对值来看，射击类游戏占比最高，休闲类与多人竞技类次之。

游戏外挂价格行情及外挂类型

对于PC端游戏，平均一款外挂的价格在15元/天，外挂以定制外挂为主，特殊定制外挂价格高达2200元/月；

对于移动游戏，平均一款外挂的价格在15元/天，特殊定制外挂价格高达1800元/月。移动游戏的外挂类型较多，包括脚本、破解版客户端、定制挂、辅助类工具、通用修改器等



相比2019年，2020年移动游戏的外挂种类主要集中在定制外挂，占所有外挂的66.4%，其次是破解版客户端（占所有外挂的25.3%）、通用修改器（占所有外挂的6.1%）、PC模拟器外挂（占所有外挂的1.2%）和脚本辅助类工具（占所有外挂的1%）。

大部分外挂为收费外挂，销售逐渐走向平台化

01/2020年外挂样本大部分由过去的免费修改器演变为收费定制挂，热门游戏收费外挂样本占到90%以上，并且集中在移动游戏中

02/外挂销售方式逐渐走向发卡网、卡盟等平台化，这些平台整合了目前外挂市场上大部分的流行外挂，逐层代理，运营成本低

03/散户制作的大部分是免费外挂，收入主要是内置广告

04/据腾讯游戏安全监测，2020年，PC端游戏大型卡盟、发卡网站数达238个，网盘数达30个；移动游戏大型卡盟、发卡网站网站数达220多个，网盘数达40个

03/游戏外挂打击的技术难点及运营难点

PC端游戏外挂

01/外挂变种频繁

外挂一日多更，自动定时发布新版本；在玩家机器上，外挂可对自身文件，内存代码添加随机数据变Hash，使得一人一外挂样本，千人千面不聚集

02/外挂实现云更新

一个登录器对应多个外挂样本，登录器自动下载功能稳定好用的外挂样本，实现云更新，即使单个外挂被对抗还有其他外挂可用，玩家持续有外挂可用，需高强度对抗

03/取证难

外挂先于游戏启动，然后将外挂核心模块以shellcode形式注入到游戏进程或系统进程中，或隐藏于第三方带签名的合法进程中（如其社交或音乐软件）。有的外挂甚至是硬件外挂（如同步器、双头盒子、鼠标宏），给全面取证、高效分析带来了难度

04/逆向难

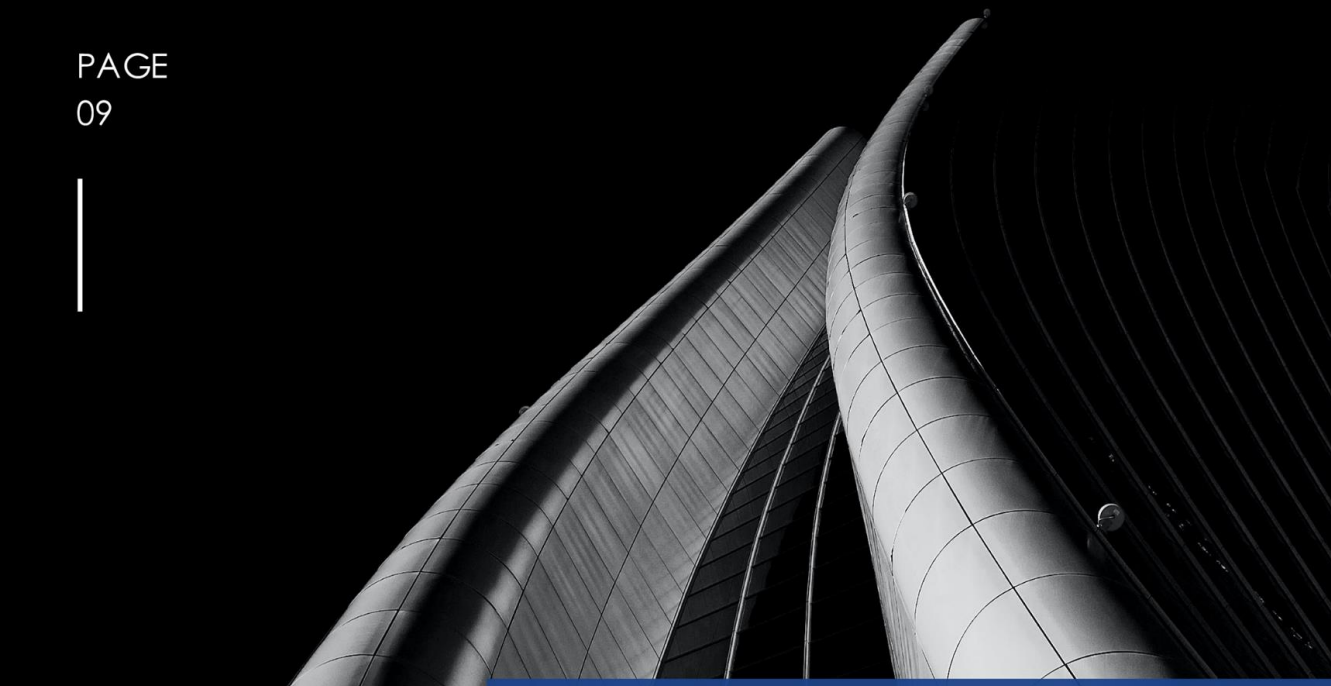
外挂核心模块关键代码使用vmprotect保护，甚至基于LLVM实现了定制化混淆保护，外挂逆向分析难度大

05/外挂在游戏内无入侵

透视、自瞄、自动连招、躲避技能等强竞技类恶意外挂无需注入外挂模块到游戏内，可通过自实现的驱动加签名或直接利用存在读写漏洞的第三方驱动获取游戏核心数据，利用AI计算替代玩家快速反应，在游戏外画框提示或使用模拟输入精准操作达到高端玩家水平，游戏内无入侵痕迹，同时很难区分是低玩作弊还是高玩正常操作

06/游戏的发展演变降低了外挂开发门槛

Unity/UE引擎加速游戏开发的同时带来引擎层通用的游戏安全风险，比如UE旁路游戏数据实现多设备透视，UnknownCheats / Github等全球开放性社区进一步加速了外挂实现的传播，降低了外挂开发门槛



移动游戏外挂

01/高定制，强对抗

随着移动游戏黑色产业链的快速成熟，部分外挂到了1天更新1-2次的频率。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

02/高维作弊

外挂作弊已经不仅是对游戏逻辑，数据的修改，或是与安全方案检测本身的对抗，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

03/伪装性强

外挂利用移动端网络流量限制，网络通信质量相对较差等特点，通过各种工具屏蔽安全方案，或是安全方案的数据传输，并模拟成网络质量不好，绕过安全方案的检测。并通过多台不同设备间互相顶号等形式。实现伪装成正常客户端的数据上报，进一步绕过安全检测

04/抗测试

目前已有部分外挂，通过对于无线wifi记录，系统缓存信息等一系列系统数据，实现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

无论是对PC端游戏还是移动端游戏，在外挂对抗的运营上，同样面临着巨大的挑战

01/玩家作弊成本低

网络上出现的各种有偿带老板上分，账号共享代练等收益大，同时黑号、小号来源多成本低，玩家无顾忌作弊处罚，进一步对游戏反外挂对抗提出挑战

02/全球化的外挂黑色产业链令打击更困难

随着游戏厂商的全球化运营布局，外挂黑产也不仅仅局限于国内市场，而开始形成分析，开发，市场，分发的跨国多团队协作的全球化形式，在黑产团伙定位上，基于政策法规的刑事打击上，变得打击更为困难

03/未知样本的对抗需求日益增长

随着各种竞技类游戏对于榜单，赛事，直播运营重点运营。玩家对于赛事榜单及直播等游戏安全性更为重视。而一般的安全对抗，基于对外挂的原理分析，并通过基于系统数据或游戏客户端数据的异常进行检测，难以有效，实时的覆盖到这种未知作弊的场景

腾讯游戏安全解决手段

面对复杂的外挂问题，腾讯游戏安全有一套成熟的对抗方案——Anti-Cheat Expert游戏安全解决方案，从客户端加固、外挂样本监控、定制外挂的检测与对抗、用户作弊处罚等360度全面覆盖外挂问题

能力项	描述	我能收获什么？
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	防止游戏出现破解版
外挂样本监控	ACE团队通过近10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	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	专业的外挂原理分析报告，及时的外挂对抗效果
安全评审	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	ACE团队根据检测结果，对游戏内作弊用户发起处罚	ACE为游戏提供分梯度的精细化处罚
误处罚投诉审核	ACE团队根据检测结果，对游戏内作弊用户发起处罚	针对玩家处罚投诉等问题，进行针对性排查，给出答复

打金工作室和游戏黑产资产

GAME BOTS AND BLACK MARKET ASSETS

01 /打金工作室帐号规模超过4980万

2020年对抗打金工作室的数据情况

	工作室对抗数据	
年 份	2019年	2020年
数 据	5480万	4980万

2020年工作室账号规模4980万,较2019年下降10%（5480w）

2021年上半年，打金工作室规模为1700万

不同游戏品类打金工作室的占比

不同移动游戏品类的黑产工作室占比

53.79% 休闲类

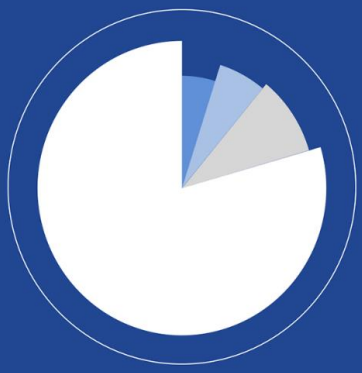
39.14% 角色扮演类

7.02% 策略类

0.05% 动作类

备注说明：射击类端游、休闲类端游及策略类端游暂无接入腾讯黑产对抗方案，暂无数据

不同PC游戏品类的黑产工作室占比



79.49%
休闲竞技类

9.5%
动作类

6.09%
角色扮演类

4.91%
多人在线战术竞技类

备注说明：射击类及多人在线竞技类移动游戏暂无接入腾讯黑产对抗方案，暂无数据

打金工作室打击难点

隐匿性变强

随着黑产技术升级 & 云手机快速发展，打金工作室的环境信息呈现越来越分散的态势，很好地将自身隐匿在正常玩家群体中。对游戏厂商精准识别的能力提出了更高的挑战

多游戏流窜

打金工作室在一款游戏上受阻后，会迅速流窜至其他游戏寻找机会，因此，单款游戏的打击还不足以阻挡工作室对游戏厂商的侵害。

获利效率高

随着对抗加强，打金工作室逐步地提高脚本打金效率，从隔天获利到小时级获利，甚至到30分钟即可获利转移。游戏厂商必须从极有限的游戏行为中，对打金账号进行快速识别快速处理，才能有效压制获利空间

游戏行为趋同

打金工作室在脚本上行为跟正常玩家逐渐趋同，会适应性地加入一些休闲玩法或社交玩家，以逃避打金行为检测。要在游戏行为上将他们跟正常玩家区分开，需要缜密精准的分析能力

2020年游戏打金工作室打金特点、变化趋势

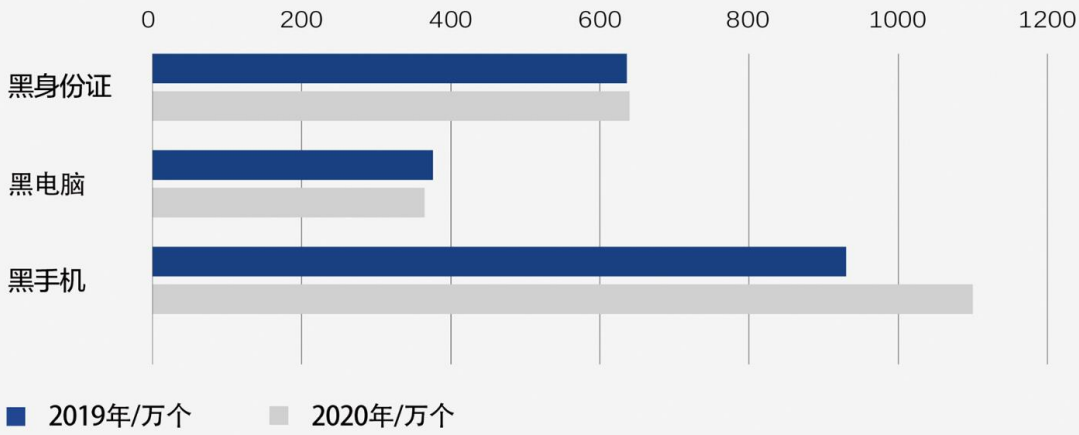
01/通过云手机&云平台进行打金的行为越来越普遍，既可以节约投入成本，又可以减少法律风险。

02/从全职工作室转向兼职工作室，或者兼职个人。个人玩家兼职打金占黑产大盘的比例逐年上升。

03/2020年，黑产通过高价收购被盗号码、利用弃游账号进行打金的行为较多，形成新的黑产账号供给产业链；同时，黑产与大R玩家形成长期合作关系，伪装成游戏内大小号的形势越来越突出。

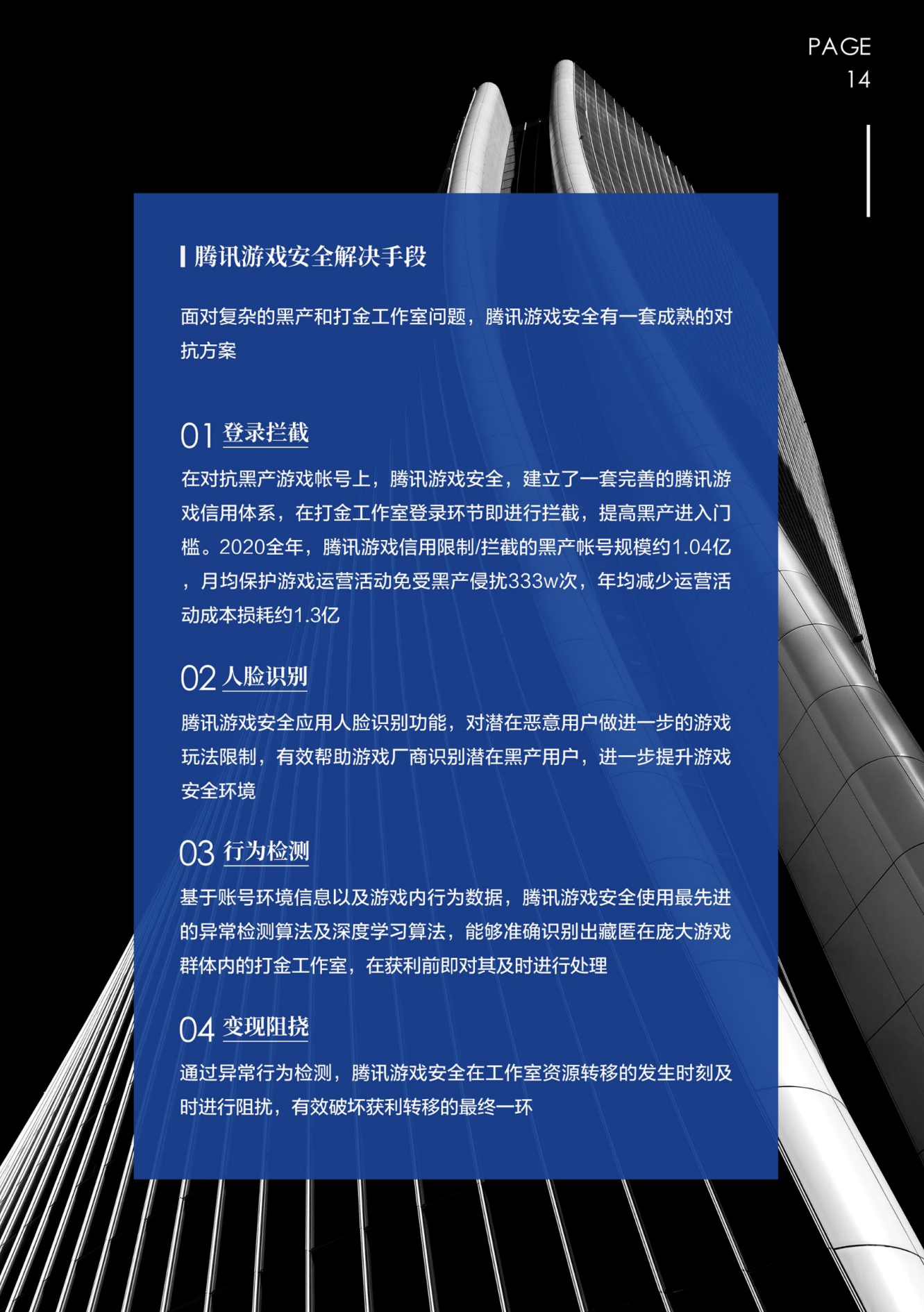
黑产手机数量快速增长

2020年据腾讯游戏安全监测，游戏黑产硬件规模价值95.2亿（2019年价值100亿），其中黑身份证640万个（价值30元/个），黑电脑353万台（价值2000元/台），黑手机1100万台（价值200元/台）



01 从数据来看，虽然整体黑产规模有所收敛，黑产PC数量减少，但随着手游规模的进一步扩大，黑产手机数量快速增长18.28%。

02 2021年上半年，因腾讯游戏安全的登录拦截方案起效，黑身份证的的数量下降至610万个。与此同时，黑手机的数量却大幅上涨，上半年涨至1700万台。



腾讯游戏安全解决手段

面对复杂的黑产和打金工作室问题，腾讯游戏安全有一套成熟的对抗方案

01 登录拦截

在对抗黑产游戏帐号上，腾讯游戏安全，建立了一套完善的腾讯游戏信用体系，在打金工作室登录环节即进行拦截，提高黑产进入门槛。2020全年，腾讯游戏信用限制/拦截的黑产帐号规模约1.04亿，月均保护游戏运营活动免受黑产侵扰333w次，年均减少运营活动成本损耗约1.3亿

02 人脸识别

腾讯游戏安全应用人脸识别功能，对潜在恶意用户做进一步的游戏玩法限制，有效帮助游戏厂商识别潜在黑产用户，进一步提升游戏安全环境

03 行为检测

基于账号环境信息以及游戏内行为数据，腾讯游戏安全使用最先进的异常检测算法及深度学习算法，能够准确识别出藏匿在庞大游戏群体内的打金工作室，在获利前即对其及时进行处理

04 变现阻挠

通过异常行为检测，腾讯游戏安全在工作室资源转移的发生时刻及时进行阻扰，有效破坏获利转移的最终一环

信息安全问题

INFORMATION SECURITY PROBLEMS

腾讯游戏信息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发言场景，涉及文本、图片、视频、语音等信息载体

不同游戏类型主要面临的违规信息类型有所不同

01 射击类游戏更容易出现外挂广告和辱骂类违规信息

02 MOBA游戏更容易出现辱骂类违规信息

03 休闲类游戏更容易出现针对未成年人的违规信息

04 所有游戏类型缺乏管控时，均容易出现色情低俗及涉管控类内容

01 /语音类恶意信息风险逐渐凸显

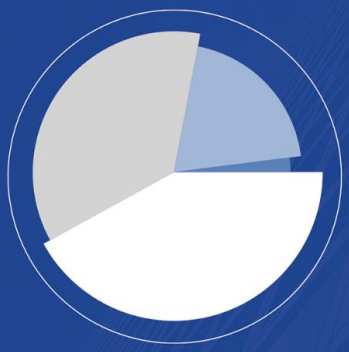
2020年，游戏业务语音场景的风险逐渐突显，腾讯游戏安全2020年在腾讯10余款游戏上线的语音审核功能，共审核61亿条语音数据，处罚量达1.6亿条；到了2021年上半年，语音审核量达到了164亿条，处罚量超过2020年全年，达3.5亿条。

02/2020年拦截恶意文本信息超过300亿条

2020年，腾讯游戏安全检测游戏内文本量为28045亿条，成功拦截掉303亿条恶意文本信息，处罚量达11亿人次；2021年上半年，检测游戏内文本量为12000亿条，处罚量达8000万人次；

2020年审核图片909亿张，打击了728万张恶意图片，累计处罚3612万人次；到了2021年上半年，审核图片950亿张，处罚量达770万人次。

2020年腾讯游戏违规信息类型



- 42% 辱骂信息
- 36% 引流广告
- 20% 色情低俗
- 2% 其他敏感信息

03/违规信息的传播更加隐晦

违规信息问题在休闲竞技类游戏上尤为突出，通常出现的违规信息类型包括

黑产广告　色情信息　诈骗信息　辱骂信息　招募引流广告信息　其他违规信息

随着腾讯游戏安全团队对违规信息的识别技术的提升，违规玩家在发布违规信息时也采用更加隐蔽的方式，如利用玩家的个性签名等叫深层的信息获取入口进行曝光。

另外，随着游戏内陌生人社交场景的发展，游戏黑产甚至盯上了一些特殊群体，如未成年人、高龄玩家等。利用特殊群体鉴别信息能力较弱的特点，对其发布特定信息以达到特定目的。

沙盒游戏、DIY类的玩法逐渐成为流行趋势，这类玩法因具有较高的自由度，也需要游戏厂商对各类型的信息加以严格审核。

04/腾讯游戏安全的应对方案

2020年，腾讯内容安全团队深耕细作，方案服务化全面升级：

01/言语辱骂方案

2020年对新出现的肺炎辱骂、地域黑、辱华3类新型辱骂类型，安全团队结合新辱骂类型的特点，定向扩充样本，快速构建检测方案，其中辱华方案接入全业务后，全业务检测量下降50%

02/色情文本方案

基于色情的定义标准，结合主动学习技术扩充样本多样性，累积标注百万条样本；同时增强方案抗变种能力。目前色情方案日均检测42.6万条，准确率95%+

03/通用诈骗引流文本方案

对网络黑产引流方式进行梳理和定义，主动挖掘拓展字母和数字变种，使用通用的预处理机制对样本变种干扰对抗，重点游戏资源广告接入通用方案后，资源广告检测效率提升2.5倍,外网恶意整体广告占比下降60%

04/UGC通用广告图片方案

2020全面提升全文字广告风格模型、美女招嫖风格模型、图片广告文本判定模型、对抗性文字区域检测模型与对抗性文字识别算法能力。方案更新后在业务对抗中的准确率提升8%

05/语音审核模式全面升级

从单一的举报审核模式逐步切换为业界领先的全量审核模式，在保证审核成本可控的前提下，全面提升审核覆盖面，对于之前未被举报的恶意语音内容也纳入了审核范畴。同时，标准化游戏语音接入模式，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

游戏云上安全问题
GAME SECURITY PROBLEMS ON CLOUD

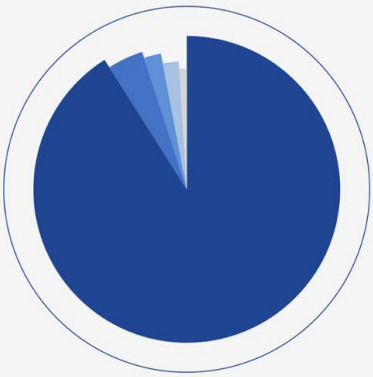
01/2020年游戏行业DDoS攻击次数创

据腾讯安全《2020年DDoS威胁报告》，2020年，游戏行业DDoS攻击次数创新高，占全行业攻击次数的79%

游戏行业攻击次数和占比走势

02/10%的游戏厂商在一个月内检测到过木马攻击

30天内恶意木马检测结果统计



91%
未发现恶意木马

4%
15天内发现恶意木马

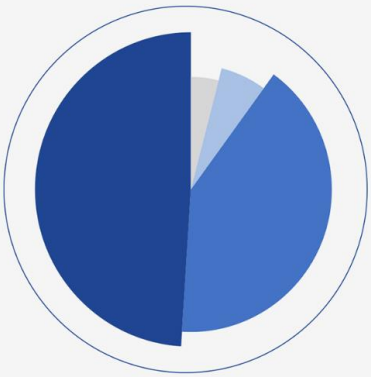
2%
7天内发现恶意木马

2%
3天内发现恶意木马

1%
30天内发现恶意木

03/59%的游戏主主机近30天内曾发生异常登录

30天内异常登陆情况统计



49%
30天内发现异常登陆

41%
未发现异常 登陆

6%
7天内发现异常登陆

4%
15天内发现异常登陆

异常登录次数最多的端口为22，占比超过70%，异常登录次数量级达每月千万次。22为远程登录服务默认端口，其他为各厂商自定义的服务端口。异常登录中最为常见的用户名为work、root和game，登录次数每月高达数百万次，常用用户名存在异常登录的占比超过85%，其他自定义的用户名则显著低于常用用户名。

04/69%的游戏厂商云主机在30天内遭遇爆破攻击

30天内云主机遭遇爆破攻击的情况

- 63% 30天内发现爆破攻击
- 31% 未发现爆破攻击
- 5% 15天内发现爆破攻击
- 1% 7天内发现爆破攻击

游戏厂商云主机在30天内曾经遭遇爆破攻击的比三分之二还要多（占69%），检测数据反映出业务系统避免使用弱密码对安全有多重要。爆破攻击次数最多的端口为22和3389，均为远程登录服务的默认端口，爆破次数每月达数十亿次，这两个端口被爆破攻击的占比达到98%，其他自定义的服务端口被爆破的次数显著小于使用默认端口。由此可见，业务系统使用自定义的端口号，就可以大幅减少爆破攻击风险。

爆破攻击常用的用户名为root、admin和administrator等常用的系统默认用户名。默认用户名被爆破的次数达到每月数亿次到数十亿次，占比超过85%。使用自定义用户名，被爆破攻击的次数显著少于常用的默认用户名。

05/54%的游戏企业在3天内发现存在漏洞风险

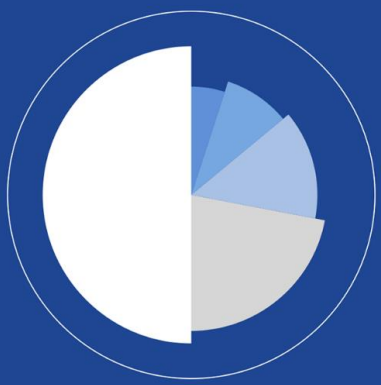
游戏行业30天内发现存在漏洞风险的情况

- 54% 3天内发现漏洞风险
- 25% 未发现漏洞风险
- 8% 15天内发现漏洞风
- 7% 7天内发现漏洞风险
- 6% 30天内发现漏洞风

高达54%的企业在3天内发现存在漏洞风险，意味有较多企业存在漏洞风险没有及时修复。一个月未发现漏洞风险的占比仅25%，积极修复安全漏洞的系统管理员不占多数。该数据提醒安全运维人员需要更加积极的响应安全漏洞告警，避免云上资产沦为黑客攻击目标。

06/50%的游戏厂商云主机在一个月内执行危险命令

云主机30天内高危命令执行情况



- 50% 未发现高危命令执行
- 22% 3天内发现高危命令执行
- 14% 7天内发现高危命令执行
- 9% 15天内发现高危命令执行
- 5% 30天内发现高危命令执行

高危命令有可能是黑客入侵之后，进一步执行恶意操作时执行的命令，也有可能是运维人员在日常操作时候执行的风险命令。需要运维人员针对高位命令的执行进行重点关注，及时研判是否是主动执行，高危命令审计对发现服务器潜在风险有着十分重要的意义。

游戏盗版问题

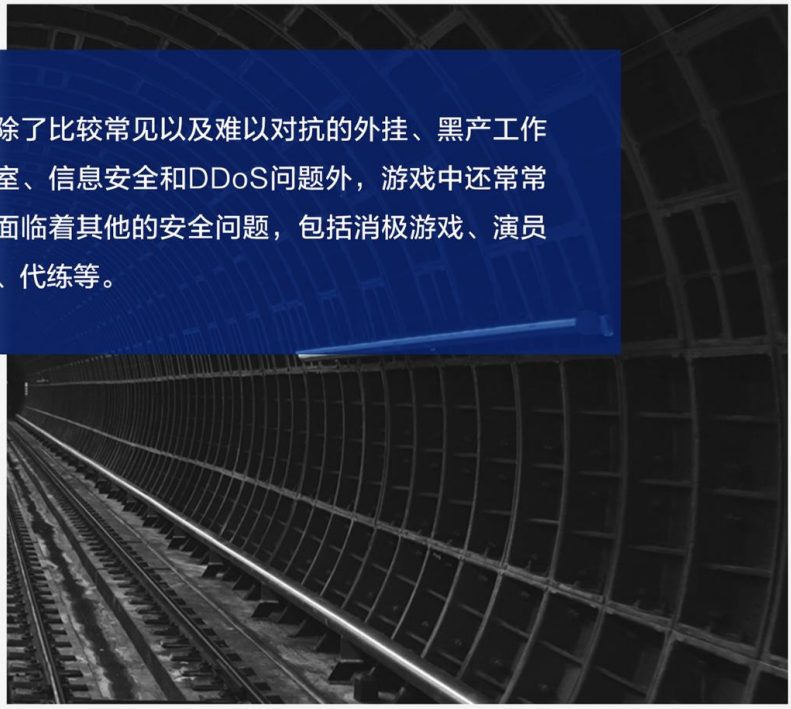
GAME SOFTWARE PIRACY PROBLEMS

游戏盗版问题通常发生在单机游戏上，单机游戏由于没法持续联网，产品上市后，就几乎没办法改变加密的模式和内容，如果没有强有力的安全保护方案，要破解就相对容易。一旦游戏被破解，使用传统的法律维权手段门槛高，取证难，周期长，很多的游戏厂商都束手无策。

使用Anti-Cheat Expert 的数字版权保护方案对客户端进行加固和保护，与发行平台进行深度绑定，不但有效校验用户的合法性，同时通过随机校验的方式防止非法破解版本扩散。

基础防护	反盗版	防扩散
具有传统加固的所有功能	与游戏发行平台深度结合	客户端与设备绑定
根据引擎类型选用加固方案	有效鉴定账户合法性	设备指纹反模拟
代码混淆、数据加密	支持主流发行平台	合法账户切换设备无感知
反调试、反重打包	支持无平台发卡模式	游戏全程随机核验
反注入、反DUMP		
S0/EXE强力加壳		

其他游戏安全问题
OTHER GAME SECURITY PROBLEMS



除了比较常见以及难以对抗的外挂、黑产工作室、信息安全和DDoS问题外，游戏中还常常面临着其他的安全问题，包括消极游戏、演员、代练等。

01 /消极游戏行为

消极游戏行为通常包括挂机、送人头。据腾讯游戏安全统计，在合作竞技类游戏中，30%以上的对局中，都存在消极游戏的问题，影响玩家数量极为广泛。

消极游戏行为的成因较为复杂，既与游戏本身的匹配机制相关，同时跟玩家自身的游戏素养有关，游戏厂商赢尽可能合理化匹配机制的同时，引导玩家积极应战，同时出台相应的处罚机制。

02/帐号安全问题

随着游戏厂商安全技术的提升，要获得一个较高等级的游戏帐号需要付出较高的成本，但很多游戏玩家却希望能够在短时间内获取一个高等级游戏账号，于是催生了越来越多的租号平台。黑产通过租号平台、借号、或者盗号等方式获取正常玩家账号，进行游戏作弊以此获利。

游戏帐号交易产业链条展示图

通过帐号交易，容易衍生出不同的游戏安全问题

帐号安全保护措施

游戏核心玩法场景身份验证：通过人脸验证、异常登录拦截的方式，提升被盗帐号的使用难度

建立被盗申诉功能，帮助被盗号的玩家找回帐号

03 积极宣导科普，增强玩家防盗意识和租号风险意识

03/游戏演员行为趋向隐蔽，并延伸至博彩领域

演员行为一般指的是“送分”与“吃分”双方玩家，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。

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，当前的演员行为日趋隐蔽，除了传统的的送分吃分行为外，还出现了专门针对头部游戏主播或者职业玩家，从而操纵比赛结果，进而参与博彩外围获利的演员行为。

MOBA博彩演员展示图

MOBA博彩演员的账号特点:

01 匹配到主播对局，多个演员操纵对局

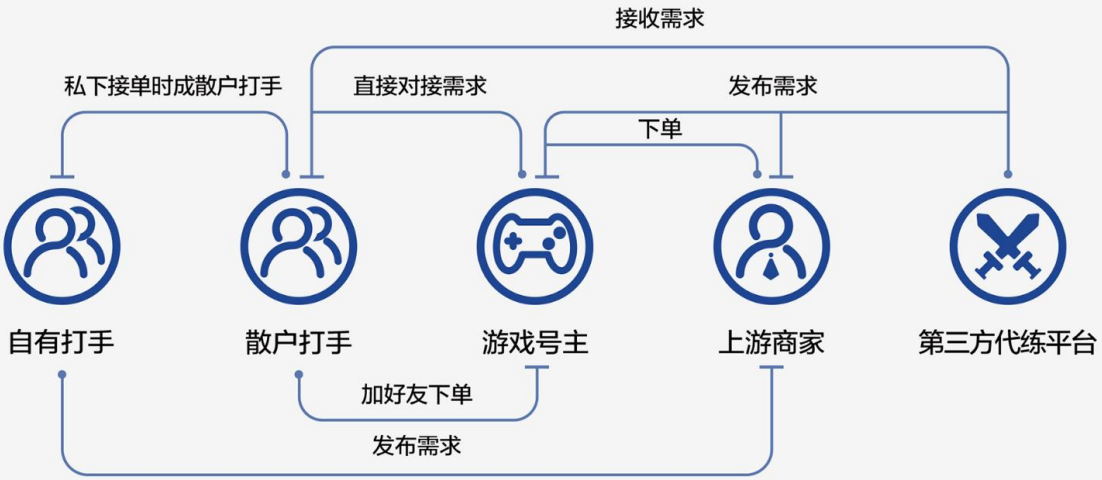
02 演员通常采用多赛季正常活跃账号，账号过去无类似的违规行为

04/玩家为刷取游戏活动奖励找代练

随着MOBA游戏新模式新玩法的普及，玩家找代练，除了以提升段位和榜单排名为目的以外，有的还会以刷取游戏活动奖励为目的。

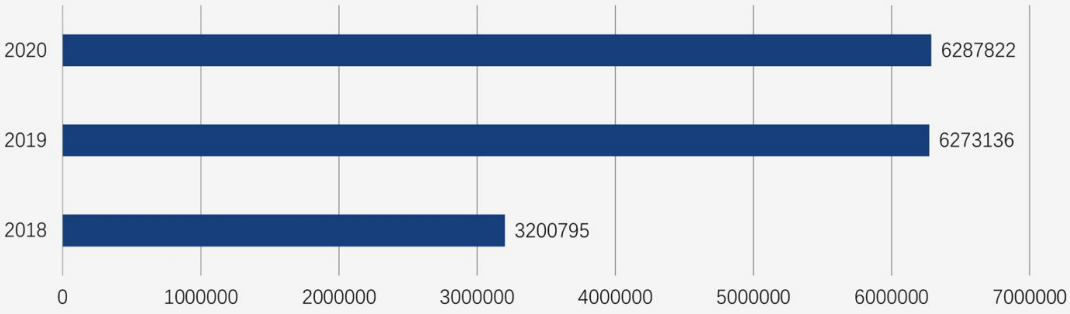
当前游戏代练产业发展成熟，网络上各种的代练中介平台和被利益驱动的代练打手越来越多， 号主、上游商家、打手、代练平台之间已经形成了一条完整的黑产产业链。

黑产产业链



据统计，2020年国内主流代练平台的发单量与2019年相比稍有上升，全年发单总量超过了600万单

主流代练平台发单



05/ 演员行为对抗手段

面对日趋隐蔽的演员行为，腾讯游戏安全建立了一套完备的演员行为打击框架，从拦截演员到KOL游戏对局监测再到官方打击信息披露等全方位出击，减少演员行为的出现。

演员行为打击框架

博彩网站	梳理核心场景	现场干预处理
01.演员剧组关系链挖掘打击团伙	01.博彩网站/APP收集	01.盘口KOL对局异常行为自动监控告警
02.对局匹配干预机制	02.博彩网站每日开盘信息统计	02.游戏内举报受理
03.狙击目标匹配行为检测	03.博彩开盘目标监控	03.视频审判处罚

06/ 代练行为对抗手段

由于代练的目的明确，通常是为了上分或刷奖，因此基于游戏帐号在游戏内的一场游戏表现，对局行为、奖励收益、上分特征等数据，腾讯游戏安全团队有着一套独特而准确的代练检测模型，帮助游戏准确识别代练帐号。

代练检测:针对不同代练目的及特点检测

01
代练上分
基于异常游戏表现+上分特点检测

02
代打刷奖
基于异常游戏环境+对局行为+奖励收益

另外在管控手段上，针对不同程度的代练行为，腾讯游戏安全也设置了多种处罚梯度。同时，做好玩家触达，形成良好的引导作用。

07/消极游戏行为应对手段

除了演员和代练，挂机、送人头、、辱骂、消极比赛等行为，也给玩家的游戏体验带来了程度不等的伤害，尤其是在团队竞技游戏中，游戏平衡性越好，这些恶意行为的发生对核心玩家带来的打击越重。需要持续修补玩法规则漏洞，定义违规行为边界和违规处罚红线，不断打击负面行为和鼓励正向良性游戏行为，保持核心玩家对游戏公平性的信心。

对此，腾讯游戏安全团队在局前、局中和局后都有着对应的应对手段，最大限度地维护游戏环境。

	检测判定系统	信誉分+处罚系统	用户触达系统
局前	消极行为分类 判定规则迭代	信誉规则展示 信誉分核实 惯犯模式拦截	信誉分过低提醒 禁模式处罚通知
局中	挂机检测 辱骂检测 逃跑检测 送人头检测	违规行为记录 恶意发言屏蔽	消极行为警告 禁模式处罚通知
局后	举报数据收集 检测数据汇总 处罚投诉反馈	信誉分扣减/恢复 消极惯犯封号	信誉分变动/封号通知 处罚公示/文章/直播引导

Anti-Cheat Expert

关于Anti-Cheat Expert

腾讯游戏安全Anti-Cheat Expert安全服务方案是基于腾讯十余年的游戏安全对抗技术沉淀和经验积累，形成的一套全面的、不断升级的、能力行业领先的安全服务产品，旨在为游戏行业提供安全服务产品，解决游戏安全问题，提升腾讯游戏安全行业内影响力。这套对外服务产品已经在腾讯运营的众多游戏海量用户级别上验证过，并将继续向行业内多家游戏公司输出安全能力，让游戏玩家体验升级，携手游戏厂商共建游戏安全健康生态，营造更具公平性、竞争性的游戏环境。目前该方案已经开放免费试用中，欢迎广大游戏厂商关注Anti-Cheat Expert 的官方微信公众号，联系官方试用，并及时获取最新的游戏安全干货。

Anti-Cheat Expert微信公众号二维码

腾讯安全微信公众号二维码

Anti-Cheat Expert 合作厂商

Anti-Cheat Expert赋能众多游戏厂商，包括Riot、Garena、Activision、Netmarble等众多公司的数百款精品手游提供了安全保护。如有需求，欢迎与我们联系。

RIOT GAMES
Garena
ACTIVISION
CALL·DUTY
miHoYo
华益天信 INFI-ENERGY
netmarble
鹰角网络 HYPERGRYPH
光爪网络
心动网络
37手游
乐逗游戏 IDREAMSKY GAMES
巨人网络
4399游戏
英雄互娱 ENTERTAINMENT
猎豹移动
SUNBORN散爆
飞鱼科技
抱一网络
库洛游戏 KURO GAME
无端科技 WZAD GAMES
KRAFTON GAME UNION
COCONUT ISLAND

游戏安全白皮书

GAME SECURITY WHITE PAPER