



图片：《绝地求生：大逃杀》

## 主播开挂被戳穿后，为何能屡次理直气壮地不承认？



游研社

是什么给了他们底气？是一条外挂产业链。

文 / Will

卢本伟凉了。

从 11 月 28 日霸气 29 杀，再到 12 月 8 日道歉停播。在这次史无前例的狂欢中，卢本伟经历了人生中最窘迫的 11 天。曾经的斗鱼一哥变成了落水狗，每个人都恨不得踩上一脚。

但重新回顾这次事件，却到处透着一股违和。把时间推回到几个关键节点就会发现，卢本伟一直都很有底气，尤其是在“自己不会被封号”这一点上，有种迷之自信。

我们都知道，确定某人是否开挂，官方封禁的确是最有说服力的。在魔音糯米开挂事件中，比起网友抬出的各种“实锤”，最终起到决定作用的依然是官方封禁。可这次，蓝洞却始终没有发声，已经被锤烂的五五开依然抱住这最后一根救命稻草，坚称自己从未开挂。

是蓝洞跟斗鱼有 PY 交易，在保着五五开吗？还是说人家卢本伟根本就是个天才，观众冤枉他了？不过这件事背后还真没那么复杂，因为就算他真的开挂了，蓝洞也很难查得出来。

外挂是如何工作的

要解释这个问题，就不得不讲一讲外挂的原理了。每款网络游戏都由客户端和服务端组成，玩家通过客户端输入操作，服务器接收操作信号后进行运算，再将运算结果反馈回客户端，最终变为玩家眼前的游戏画面。

理想状态下，数据应该由服务器决定，客户端只负责显示结果。但是 FPS 游戏都存在延迟问题，不可能在开枪之前先通过服务器验证信息，只能把很多运算放在本地进行，这就给了外挂可乘之机，只需要绕过反外挂机制，调出本地数据，就能够实现各种外挂功能。

最简单的外挂会直接修改输入数据，我们一般称之为内存挂。内存挂简单粗暴，能够实现一些匪夷所思的功能：



改变角色坐标，就能飞天遁地



改变角色骨骼参数，可以变成路飞



改变敌人的角色坐标，使出吸星大法

这些看似很强的内存挂其实并不专业，它们会留下无法清除的异常数据，反外挂程序可以轻易追查。所以“神仙斗法”型外挂都是一次性用品，惨遭

封号是迟早的事。除了《绝地求生》，我们很少会在其他游戏中见到这类外挂。

更主流的外挂不会修改数据，只需读取游戏内存或模拟玩家操作，就能让开挂者获得巨大的优势。这类外挂技术要复杂一点，但是对于大多数反外挂程序来说，它们无迹可寻，追查起来难度很大。

比如透视功能就是利用了读取内存的技术，将本该对玩家隐藏的坐标信息显示出来。



至于降低后坐力的压枪挂，是通过虚拟指令，模拟鼠标的移动轨迹，开枪之后把准星迅速定位到原来的位置。

```

        VOID mouse_event(
            DWORD dwFlags, //鼠标动作标识。
            DWORD dx, //鼠标水平方向位置。
            DWORD dy, //鼠标垂直方向位置。
            DWORD dwData, //鼠标轮子转动的数量。
            DWORD dwExtraInfo //一个关联鼠标动作附加信息。
        );

```

其中，dwFlags 表示了各种各样的鼠标动作和点击活动，它的常用取值如下：

MOUSEEVENTF\_MOVE 表示模拟鼠标移动事件。

MOUSEEVENTF\_LEFTDOWN 表示模拟按下鼠标左键。

MOUSEEVENTF\_LEFTUP 表示模拟放开鼠标左键。

MOUSEEVENTF\_RIGHTDOWN 表示模拟按下鼠标右键。

MOUSEEVENTF\_RIGHTUP 表示模拟放开鼠标右键。

MOUSEEVENTF\_MIDDLEDOWN 表示模拟按下鼠标中键。

MOUSEEVENTF\_MIDDLEUP 表示模拟放开鼠标中键。

这是外挂教程中，一段模拟鼠标指令的代码

自瞄结合了以上两种功能，先读取内存，找到其他角色的骨骼位置，再模拟鼠标操作，让枪口始终跟着人物骨骼模型。自瞄可以爆头，当然也可以固定瞄准其他位置，“超级瞄准”部署之后想打哪就打哪。



黄线就是人物骨骼



开了自瞄之后我自己都控制不住自己

成功绕过内存保护后，模拟鼠标信号在程序看来就和玩家操作就没什么区别了，反作弊程序很难监控到非内存挂的存在。剩下的唯一方法和杀毒软件类似，就是在游戏启动时扫描后台程序，将外挂精确识别出来。

可是该如何识别出哪些程序是外挂，同时又不误封正常程序呢？

要想找到外挂，需要通过一个叫做“**特征码**”的东西，每种程序都拥有一段特征码，这相当于程序的指纹。只要得到外挂的特征码，游戏运行时反作弊程序就能确认玩家是否开挂。

这也意味着，想要找到外挂，至少需要一个样本。为了获得外挂特征码，游戏厂商和外挂贩子每天都在上演着“无间道”。官方会用各种方法获得外挂样本，比如派出卧底购买外挂。拿到样本后，通过技术手段分析它们的特征码，才能将同种挂全部封禁。

外挂贩子则会做出很多种功能相同而特征码不同的外挂，将客户分为几十人或上百人一个小组，哪个小组被封了，哪里就出了内鬼。之后可以通过重新分组等方法快速追查到卧底，把二五仔送进黑名单，永远不再提供服务。

在不断的斗争中，反作弊程序始终处在下风。但外挂贩子的制售成本也一直在攀升，过去一个外挂可以卖给几百上千人，现在只能卖给几十个人，所以你可能还惊讶于吃鸡外挂的价格，供需关系导致了它的高价。

进一步地，如果找不到样本，那反作弊程序就无计可施了。要是你愿意掏更多的钱，一个人把这几十个人的钱都出了。那么恭喜你，你将拥有一款主播专用定制挂！它的特征码全球独一无二，即使你用到吃鸡关服，官方也拿你没办法。面对任何质疑你的人，都可以用一句话搪塞过去——“蓝洞没封我的号，所以我没开挂。”

### 无可奈何的蓝洞

蓝洞真的束手无策了吗？至少目前看起来是这样的。

《绝地求生》作为一个韩国小厂的作品，遏制外挂的能力明显低于业界平



均水平，在外挂同样泛滥的其他 FPS 游戏中，很少会流传出来飞天遁地骨骼变形这么离谱的外挂，这说明蓝洞连最基本的代码可能都没写好。这款“虚幻 4”打造的游戏仅用了一年时间来完成开发，很难想象程序中到底存在多少漏洞。

不过在外挂的设防上，蓝洞其实也曾努力过。《绝地求生》使用了最激进的反外挂程序 **BattlEye**（后文简称 **BE**）。一些玩家可能都听说过 **BE** 曾经逼死了《方舟：生存进化》的外挂制售团队，可能也知道 **BE** 拯救过曾经群魔乱舞的《彩虹六号：围攻》。至少在目前来说，市面上没有比 **BE** 更好的第三方反作弊程序了。



使用 **BE** 反外挂的游戏

对于外挂制作者，**BE** 也是最令他们感到棘手的東西，破解 **BE** 的成本要远高于其他反挂程序。据一位网友整理，在外网上明码标价的《绝地求生》外挂，均价在每月 150 美元左右，而一款《CS:GO》外挂有的仅需 10 美元。

除了使用 **BE** 反外挂程序，在完善自身漏洞上，蓝洞也算得上不遗余力。无论是更新还是封禁都相当频繁。在新地图中加入的死亡回放功能，似乎也表明人工监管力度会越来越强。

只不过人手太少，窟窿太大。就算蓝洞更新得再快，**BE** 功能再强，在无数条隐秘的生产线上，外挂还是在源源不断地被生产出来。

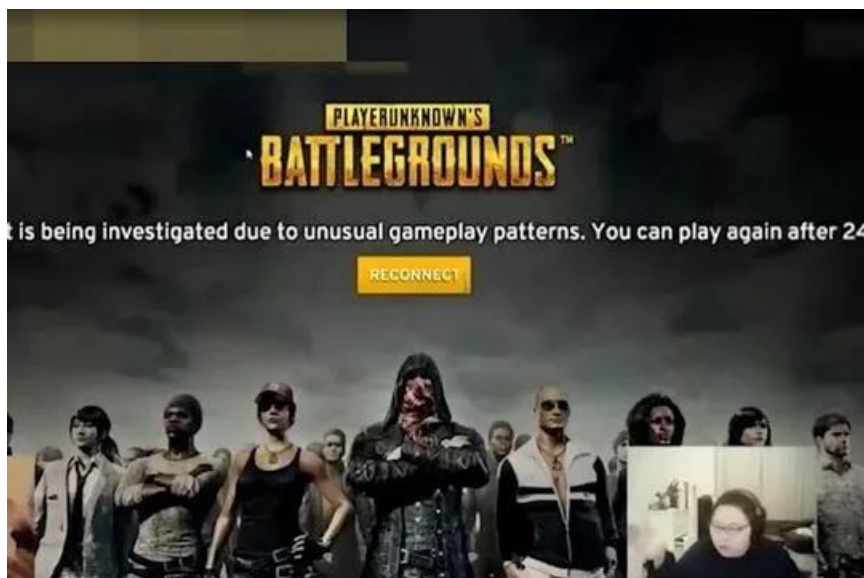
对于一款成熟的射击游戏来说，治理外挂往往需要多管齐下。比如《CS:GO》和《彩虹六号：围攻》这两款游戏，在程序反挂的同时，也使用社区

GM 监管。一旦有些玩家战绩过高，或遭到多次举报，就会触发监管机制。将被举报者的录像发给一些拥有监管权限的玩家，并由他们判断被举报者是否开了外挂，进一步压缩开挂者的生存空间。



### CS 的监管模式

《绝地求生》其实也尝试引入了这种机制，一局击杀超过 15 人或被多人举报，会将嫌疑账号封禁监测，PDD 就因一局 17 杀吃鸡而被封号 24 小时。



但目前来看，这种方法还没有全面实施，以《绝地求生》的玩家基数来看，推行人工监管依然需要很长的时间。讽刺的是，《绝地求生》引以为豪的游戏设计，也给外挂留下了很大的发展空间——只需要简单的透视和压枪，就能获得巨大的收益，每局一百人只有一个胜者的游戏模式，让开挂者获胜后能获得极大的成就感。



















相应的，主播开挂的动机也就更为强烈了：作为一个极其推崇个人英雄主义的游戏，能经常吃到鸡的技术型主播，可以收获大量的关注度和崇拜者，这些都与主播的收入直接挂钩。花钱卖挂开直播，然后赚更多的钱，

这就是开挂主播的盈利模式。

外挂从哪来？

《绝地求生》获得了与其量级不相匹配的成功，接踵而来的许多问题，并不是蓝洞这家小作坊处理的了的。更别提还有一群虎视眈眈的人眼馋着这块肉。由于利益驱使，外挂贩子也迅速地团结了起来，这个团体的规模可能比整个蓝洞还要大。

国内外的一些专用论坛，就成为了外挂贩子的根据地。这里简直是外挂开发者的天堂，不仅可以公然叫卖外挂，甚至还有一股子学术氛围。这些黑客看起来都是专业的程序员，活跃度非常高。他们还会交流技术，请教问题，共享外挂源码，你甚至可以找到教新手做外挂的教程，气氛好得有点诡异。

Threads in Forum : Playerunknown's Battlegrounds	
	<b>Announcement:</b> <a href="#">Moderators needed</a>
	<b>Announcement:</b> <a href="#">Support the community by contributing to the Wiki for this section!</a>
Thread / Thread Starter	
	<b>Sticky:</b> <a href="#">[Coding] Structs / Offsets</a> (  1 2 3 4 5 ... <a href="#">Last Page</a> ) KingRain
	<b>Sticky:</b> <a href="#">Play Together Thread</a> (  1 2) Sticky
	<b>Sticky:</b> <a href="#">[Information] Now main exe packed with Themida</a> (  1 2) MrPTFO
	<b>Sticky:</b> <a href="#">Complete Hack &amp; Tool List</a> Sticky
	<a href="#">[Help] Nograss?</a>  <b>LIVE TOPIC</b> Ropser69
	<a href="#">Help me PAK</a>  <b>LIVE TOPIC</b> masterkeys921
	<a href="#">[Release] No Recoil + Gold Players .PAK mods</a> (  1 2 3 4 5 ... <a href="#">Last Page</a> )  <b>LIVE TOPIC</b> dracorx
	<a href="#">[Release] No Walls .PAK Mod</a> NullException
	<a href="#">[Question] Bullet Drop</a> jo282

这是国外最大的外挂论坛之一，他们什么外挂都做，几乎无所不包  
做外挂的也可以很八卦，他们也会讨论五五开同学：



## About a china game anchor LuBenwei

LuBenwei is a famous china game anchor in douyu.com.

Recently it's a hot thing in China. One person suspected that he cheated and analyzed the suspicious operation in his live broadcast. But he denied cheating and incited fans to attack him.

For he's 29kill video and more video, I think he is use ESP,Aimbot,NoRecoil, I want to know if you think he cheats or not?

He's account:

<https://pubg.op.gg/user/Lu>

<https://pubg.op.gg/user/id>

<https://pubg.op.gg/user/ni>

He's 29 kill live video:

<https://www.youtube.com/>

卢本伟是一个非常出名的中国主播，一个人认为他用了外挂，并分析了他的各种操作，但是卢本伟不承认自己用了外挂，还发动粉丝攻击那个人。

看了他29杀吃鸡的视频，我觉得应该是用了透视、自瞄和减后坐力，你们觉得他开挂了吗？

最后这些做外挂的人居然还得出一个结论，说五五开可能没开挂，只是用了鼠标宏。



比起平淡无奇的国外论坛，国内外挂论坛的画风则是一片热闹，红红火火。

这里不仅可以卖挂，还能招聘、找项目、招投标。单刀直入绝不墨迹，整个流程非常“效率”。

<b>绝地球求生来个实力作者吃肉项目!!!进来加q</b> [预算1~50交易币 / 还需1投标]	19天后截止
雇主: q573422192	2017/12/11
<b>绝地项目招收子代理,吃肉项目!</b> [预算1~50交易币 / 还需1投标]	19天后截止
雇主: 860560877	2017/12/10
<b>绝地球求生 pak无后合集能过检测的来~新写法 ...</b> 投标截止	投标截止
雇主: 849519375	2017/12/09
<b>来个绝地球求生实力作者 要求不难</b> [预算1000~2000交易币 / 还需5投标]	3天后截止
雇主: 209866155	2017/12/09
<b>绝地球求生找作者定制版本</b> [预算1~50交易币 / 还需1投标]	18天后截止
雇主: So项目找合作	2017/12/08

反外挂程序不断更新换代，给外挂开发带来很大的阻碍。为了集中力量突破游戏厂商封锁，他们还会共享大量的源码和成品模块。看来只有互帮互助才能实现“共同富裕”。

<b>[辅助源码分享] 荒野行动!沐兮</b> <b>新人贴</b> @ 🍵 New
<b>[辅助源码分享] PC荒野行动【方框透视】全网首发源码</b> 🍵 🍵 ... 2 New
<b>[辅助源码分享] D3D外部绘制模块源码,自己修改创建的特征可过绝地检测</b> <b>新人贴</b> @ 🍵 ... 2
<b>[辅助源码分享] 必贴必火~~~全套源码!!!</b> 🍵 🍵 ... 2 3 4 5 6 .. 91
<b>[辅助源码分享] 青橙的一些源码新鲜版</b> 🍵 ... 2 3 4 5 6 .. 19
<b>[辅助源码分享] 你们一直想要的终结者辅助源码</b> <b>新人贴</b> New
<b>[辅助源码分享] PC荒野行动【方框透视】源码来了</b> <b>新人贴</b> 🍵 ... 2 3 4 New
<b>[辅助源码] 一款易语言远控源码!!!!</b> 🍵 ... 2 3 4 5 6 .. 21
<b>[辅助源码] 开源可以用的辅助</b> 🍵 New
<b>[辅助源码] Yetong驱动绘制开源 有模块</b> 🍵
<b>[辅助源码] 方框透视源码 - [售价 3 港币]</b> @ ... 2 3
<b>[辅助源码分享] 易语言源码与模块解析,分享一下,(破解模块必备)</b> @ New

中国的外挂贩子在开发领域也独树一帜，他们普遍使用一种“易语言”编写外挂，据说这种语言全部使用中文，门槛非常低，开发者自称“可以在很短的时间内精通”。这款相当不入流的语言，不知从何时开始变成了外挂开发的重地。很多开发者甚至说，易语言对外挂产业在中国的发展起到了至关重要的作用。

全汉语编程，简单易上手。学习易语言可在两个月甚至更短的时间内学到精通程度。

程序自带教程源码，视频，每日一贴，及时帮助等(易语言完整版)，可不用互联网，在程序自身的情况下也能很好的认识到易语言。

易语言的自我宣传

这样看来，开发外挂和反外挂的难度完全不对等。做出一款最基本的外挂，可能并不需要多高的开发水平，而一张外挂月卡竟能卖出几百乃至上

千元，实在是暴利。怪不得吸引了这么多人源源不断投入到外挂行业中。

在中国，外挂产业已经形成了一个完整的生态，这些人对游戏市场非常敏感，哪个游戏火了，他们会一窝蜂地扎进去，当这个游戏的玩家流失殆尽，他们便开始投身下一个项目。当然，私人订制也是他们的业务之一，游戏主播带来的巨大流量正在悄然改变这个灰色产业的规则。

### 关于主播

最终毁灭五五开的，不是开挂，而是膨胀。

实际上，主播使用外挂从来都不是新鲜事。就连职业选手，也出现过在众目睽睽之下使用外挂的先例。以目前的技术，游戏厂商完全无法防范最顶级的外挂。

主播使用外挂太安全了，代价太低了。在各种 6666 的打 Call 声中，有些人逐渐把自己的谎言当了真，以为开了外挂才能做到的事，也是自己的实力。最后，他们连戏也懒得演了，这才使出了 2 秒 17 发，这才大胆地 29 杀吃鸡。

开挂主播们可以一直头铁下去，自以为谁的声音大谁才有道理。因为他们知道那把封号的“实锤”永远不会落下来。但他们却忘了，把一个草根主播捧上天的，不是一款游戏，也不是直播平台，而是那些最普通的观众，但观众从来都不是任凭摆布的傻子。

就算逃过了游戏厂商的制裁，就算直播平台全程无动于衷，只要失去了观众的信任，他们拥有的一切，都是空中楼阁。

[查看知乎原文](#)

客官，这篇文章有意思吗？

好玩！[下载 App 接着看 \(๑•H•\) ♡](#)

[再逛逛吧 ' \\_ >`](#)

[阅读更多](#)

后来我才知道，「停靠在八楼的 2 路汽车」里有个地标……



[下载「知乎日报」客户端查看更多](#)