**iShot 2.3.2 破解-超级右键家族软件**

https://www.52pojie.cn/forum.php?mod=viewthread&tid=1732736

|  |
| --- |
| **更新 - 2.3.2 Pro 版本**  **一 Show Show Way**    该版本依然是start函数入口：  下翻找到：   byte\_100148D10 byte\_1001470D9 两个地址，我们要做的事情就是   1. byte\_100148D10 设为0 2. byte\_1001470D9 设为1 3. 修改主界面显示字体     **二 解决未知错误 需要重新下载**  因为byte\_100148D10被强制设为了1导致的。在iShot中byte\_100148D10=1表示有激活授权，于是他开始读取激活授权文件，这个时候就出现问题了：我不是正版用也没有激活授权文件，读取到空文件后就直接闪退了。。。  所以总结如下： byte\_1001470D9 地址在函数入口设为1即可激活。  **三 下载补丁**  仅支持Intel。 For 2.3.2 懒人一键体验布丁： 解压两个文件替换掉 /Applications/iShot.app/Contents/Frameworks/PTHotKey.framework/Versions/A/PTHotKey  总有人看不到下载地址： 下载:<https://wwsq.lanzoub.com/iJm6I0n9t6sb> 密码:52poji 体验正版可以，但是请支持正版！ 众所周知，我喜欢潜水在各大qq群，有知道我账号的千万别在群里问xxx你是吗啥的，有些群里是人家软件官方群，你这样子很不体面，人家正版软件开发者还在群里呢。。。   # 以下为 iShot 2.2.9 版本破解过程  **0 Tools**   1. IDA 8.2 Free 官网免费版本 别问哪里能下了 IDA官网 官网！！ 2. nop   **1 先看软件**    **2 分析过程**  之前超级右键看过之后我们知道他在启动函数中做了receipt授权验证 那么我们直接看start函数  换汤不换药 直接ban掉v17 jz      loc\_100064FA3 改成jnz即可 接着ban掉两个夺命连环call objc\_msgSend    修改后如图所示。     红色部分为修改后的二进制数据 用了大量的nop来跳过代码执行  上图中v23不修改的原因是只需要在下面把标志改为1即可，因为v23 == True的话结果也是将r60设为1 所以我们直接跳过让他强制设为1. 然后将else分支中的r60 = 0强制改为1  eax赋值为1即可实现订阅破解,最后走了173行处逻辑。  **3 成果** |

**免费评分**