**超级右键 2.2.1 破解**

https://www.52pojie.cn/forum.php?mod=viewthread&tid=1732659

|  |
| --- |
| **优化MacOS下的超级右键2.2.1**  **Tools**   1. IDA 8.2 Free 2. 6A 01 58 C3 3. sudo cp /Users/qiuchenly/Downloads/iRightMouse /Applications/iRightMouse.app/Contents/MacOS/iRightMouse && sudo codesign -f -s - --timestamp=none /Applications/iRightMouse.app/Contents/MacOS/iRightMouse 4. jz => jnz; nop(90);   **0x01 灵根育孕源流出 心性修持大道生**  从AppStore下载的版本如图所示。  左下角有一个订购按钮，盲猜订阅后会消失。但这并不是重点。  **0x02 悟彻汇编真妙理 断魔归本合元神**  正如上图所示，肯定要搜字符串"您的试用期还剩下xxx"啊！ 这种想法是错误的。我们看一下代码：  函数是顺序执行的，也就是说: 只有没有订阅的用户才会提示这个字符串，如果订阅了会直接不显示。 这一点我们打开start函数----也就是app入口函数佐证这一点：   注意看伪代码228行,我来翻译一下这段代码:  *复制代码 隐藏代码* if(v37){//如果v37的值非0:意思就是v37这个寄存器内有数据      v38=v37;//意义不明 反编译器的bug      v39=getUserReceipt().decryptPKCS5:WithPassword(qwordxxxx);//解密用户购买的授权文件      v42=AESEncryptUtil.dictionaryWithJsonString(v40);//转换为JSON数据给软件读取      if(v42){//如果数据不为0:指寄存器中存在数据          byte\_10003BDD8 = sub\_10001D3D4(v42) != 0;//byte\_10003BDD8赋值为1表示注册成功,意思就是sub\_10001D3D4()返回值要非0才行.      }  }  if ( byte\_10003BDD8 )//如果为1    {      objc\_msgSend(v3, "removeObjectForKey:", "LeftTime");//删除剩余时间key对应的数据 应该是类似于取消显示      byte\_10003BAA8 = 0;      goto LABEL\_47;//这里直接跳转到启动主程序代码 而不进行后面的剩余时间计算    }  想必大家都看得懂了。那么我是怎么知道这里是检查授权的呢？  答案很简单，我直接翻开入口函数就发现这段代码了。 做IOS开发的想必知道receipt这个单词的意思，虽然我对IOS开发一窍不通:这是表示读取Apple用户订阅的有效授权票。 结合上面说到的跳转，我想你也能猜到这到底代表什么意思了吧！  那么爆破点在哪里呢？  **0x03 IDA助威征正版 落叶施法灭授权**  即然知道问题在哪里,那么我们就要狠狠的Crack it。  *复制代码 隐藏代码* if ( v37 )    {      v38 = v37;      v39 = objc\_msgSend(&OBJC\_CLASS\_\_\_AESEncryptUtil, "decryptPKCS5:WithKey:", v37, qword\_10003BDE8);      v40 = objc\_retainAutoreleasedReturnValue(v39);      objc\_release(v38);      v41 = objc\_msgSend(&OBJC\_CLASS\_\_\_AESEncryptUtil, "dictionaryWithJsonString:", v40);      v42 = objc\_retainAutoreleasedReturnValue(v41);      v43 = v42;      if ( v42 )        byte\_10003BDD8 = sub\_10001D3D4(v42) != 0;      objc\_release(v43);      objc\_release(v40);      v28 = v115;    }  改为  *复制代码 隐藏代码* if ( !v37 )    {      v38 = v37;      nop;      v40 = objc\_retainAutoreleasedReturnValue(v39);      objc\_release(v38);      nop;      v42 = objc\_retainAutoreleasedReturnValue(v41);      v43 = v42;//由于nop了赋值函数 这里v41会变成0 也就是v42会变成0 所以要把jz改成jnz强制跳转。      if ( !v42 )        byte\_10003BDD8 = sub\_10001D3D4(v42) != 0;      objc\_release(v43);      objc\_release(v40);      v28 = v115;    }    也就是如图所示两个夺命连环Call。如果你不nop掉软件会因为null指针崩溃:因为你根本没有授权文件，读到的可不就是null?   黄色表示修改后的字节。  sub\_10001D3D4函数改返回值 6a 01 58 c3。  改为   即可。  最后别忘了v37也需要反转字节哦！jz改为jnz即可。  最后改完之后伪代码如下：  最后导出文件，codesign it。  打开app：   发现左下角的订购按钮已经悄然失踪。并且应该不会有暗桩，因为上面计算时间的代码此时被我强制跳过，也就是走的正版激活版本的流程。  **0x04 九九数完魔灭尽　三三行满道归根**  最后欣赏一下成品: |

**免费评分**