破解XXX游戏驱动保护过程总结

转载

weixin_34204722 于 2017-11-13 16:53:00 发布 510 收藏 1
文章标签： php
原文链接：https://yq.aliyun.com/articles/568919

刚刚接触软件破解还有驱动编写，好多东西都不熟，折腾了好久，把中间可能对大家有价值的过程记录下来。

刚开始碰到的问题就是不能内核调试，因为要写驱动，需要用到。一般禁用内核调试都是在驱动里调用KdDisableDebugger，往上回溯一个函数，基本上就是驱动检测禁用是否成功的代码，否则就是一个循环不停的调用KdDisableDebugger函数。

我的做法是修改KdDisableDebugger代码，这样不管什么时候被调用到，内核调试都不能被禁用，无非就是驱动那个死循环会导致机器卡死罢了，在KdDisableDebugger上设置一个断点，中断后，就把KdDisableDebugger和驱动的代码都改掉，然后禁用断点，继续内核的执行。我用的是下面这个命令做这段话说的事情：

bp KdDisableDebugger"eb nt!KdDisableDebugger+26 75;eb nt!KdDisableDebugger+41 75;ebTesSafe+5069 74;eb TesSafe+2703 75;bd 0;g"

然后就是把驱动里hook的函数恢复，为了找到内核ssdt表里被hook的函数，看了网上的资料，有工具可以做这个事情，一是那些工具我都没有用过，不大会用，二是我想把内核里具体被inline hook的地址找出来，所以我就用了下面这个windbg脚本做这个事情，运行脚本之前需要记下eax, ebx, ecx的值，等脚本运行完成以后恢复。当然也可以用windbg里的伪寄存器，但是语法还有点不熟，就直接用现成的寄存器了，在启动游戏之前，先dump一下：

```
.logopen c:\logs\beforehook.txt  # 因为dump出来的东西比较多，就放到一个log里
r ebx = 0                        # 计数器

# 遍历ssdt表，把里面每个函数的汇编代码都dump出来，因为不知道每个函数的大小，所以每个函数都dump 1000行。
r ecx=poi(nt!KeServiceDescriptorTable)
.for (r eax=ecx;@eax < ecx+0x474; reax=eax+4; rebx=ebx+1) { r ebx; u poi(@eax) L1000}

# 保存log
.logclose
```

接下来，游戏启动之后，再dump一次，用kdiff3做个对比就知道哪些函数被修改过了。

看到被hook的函数以后，加上网上的资料，主要是参考看雪里的这篇资料：
http://bbs.pediy.com/showthread.php?t=126802

但是悲剧的是，有的时候修改了TX的代码，机器直接就重启了，参考看雪里另外一篇文章，把重启这个问题也解决了：
http://bbs.pediy.com/showthread.php?t=129810&highlight=DNF

很多都是大侠们已经研究了很透的东西，只是我比较愚笨，花了很多时间才搞明白整个过程，完整驱动的代码可以在我这个求助帖里找到：
http://www.ghoffice.com/bbs/read-htm-tid-91059.html