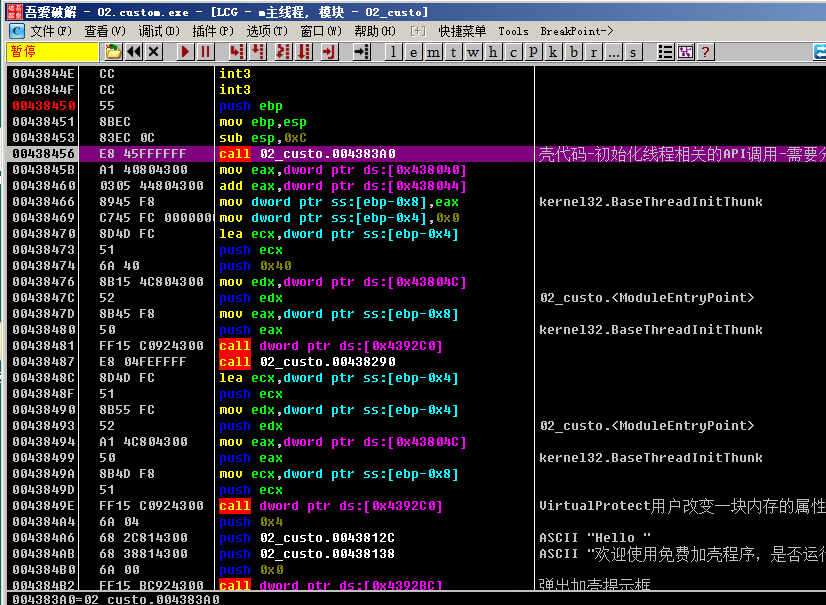
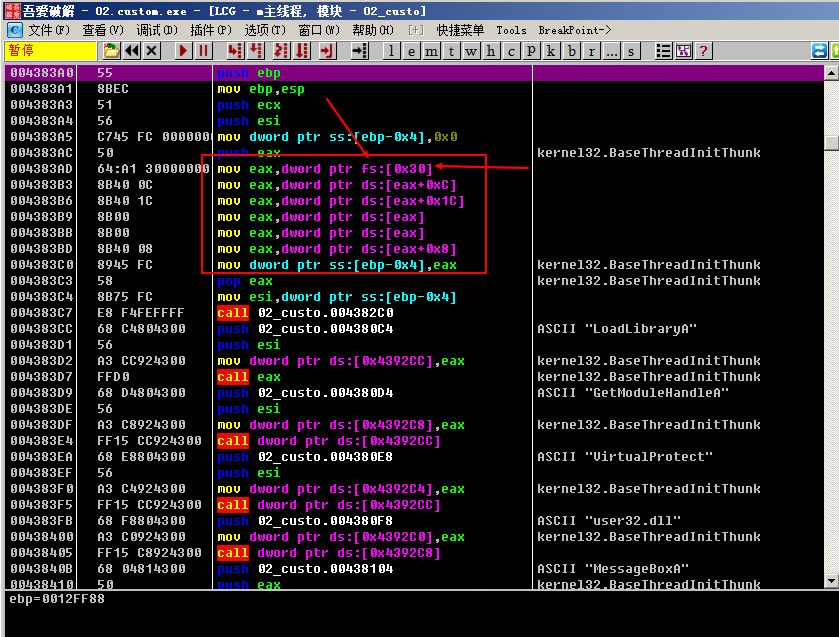
进来看到并非OEP，而且用PEID等看不到导入表的内容，为空，因此猜测这些API并非死写在导入表中，而有可能通过其他的方式获取到。



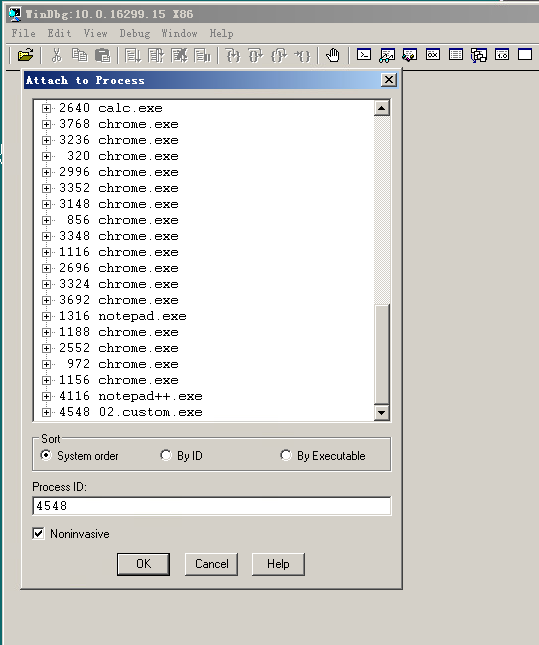
进入第一个call看看，发现熟悉的TEB到PEB的查找流程，尤其是FS寄存器的使用，这让人猜测API就是通过保存在FS寄存器中的地址获取到的。



FS寄存器：指向当前活动线程的TEB结构（线程结构）

32位机器TEB结构地址保存在FS，64位是GS

为了继续分析，在windbg中附加此程序



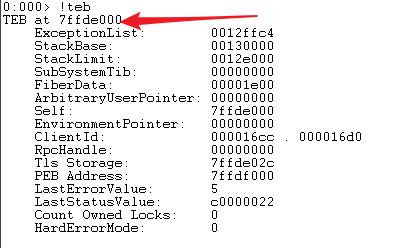
如果没加载pdb符号信息，需要手动设置一下符号下载服务器：

查看当前符号路径：.sympath

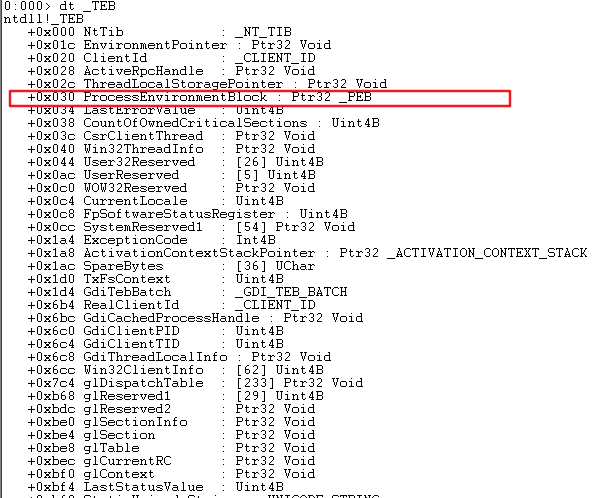
设置符号路径：.symfix d:\symbols

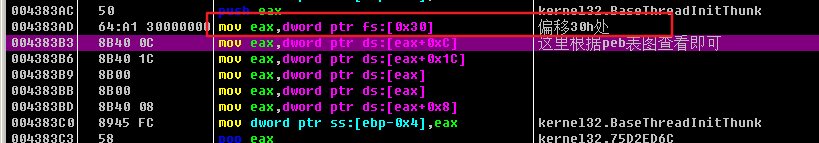
重新加载符号： .reload

设置完毕输入命令!teb查看TEB结构：可知TEB结构体的地址为7ffde000，即FS寄存器中的值为7ffde000

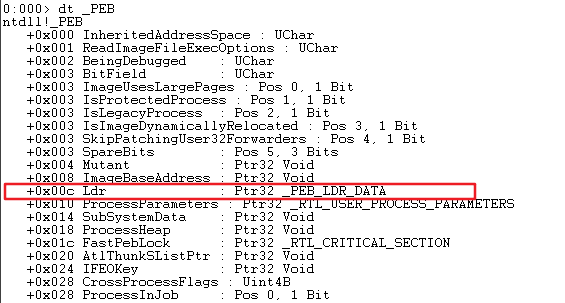


**输入dt \_TEB可以查看TEB的具体结构，可以看到0x30处指向了PEB结构**

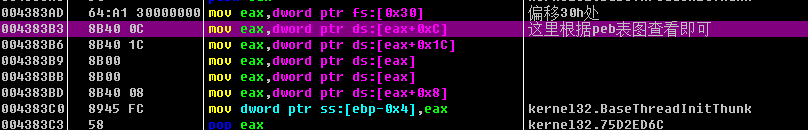


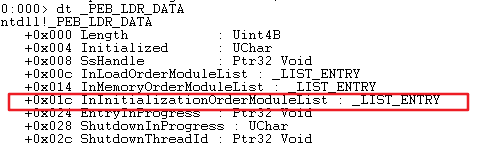


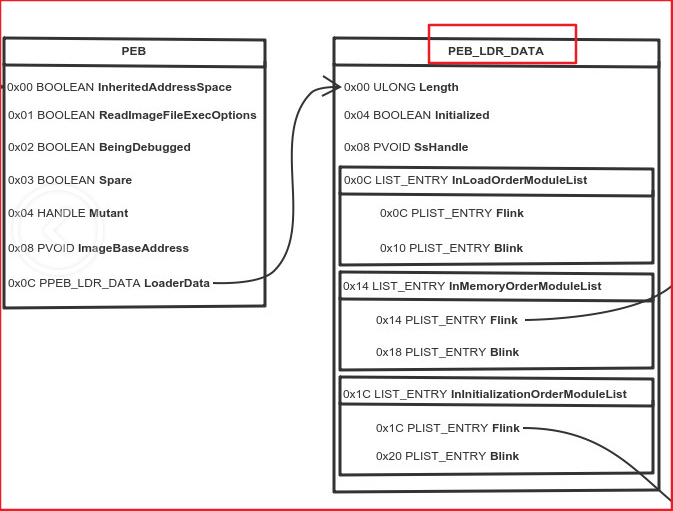
可以继续查看PEB的结构，能够看到偏移c处为Ldr，该成员为\_PEB\_LDR\_DATA结构体



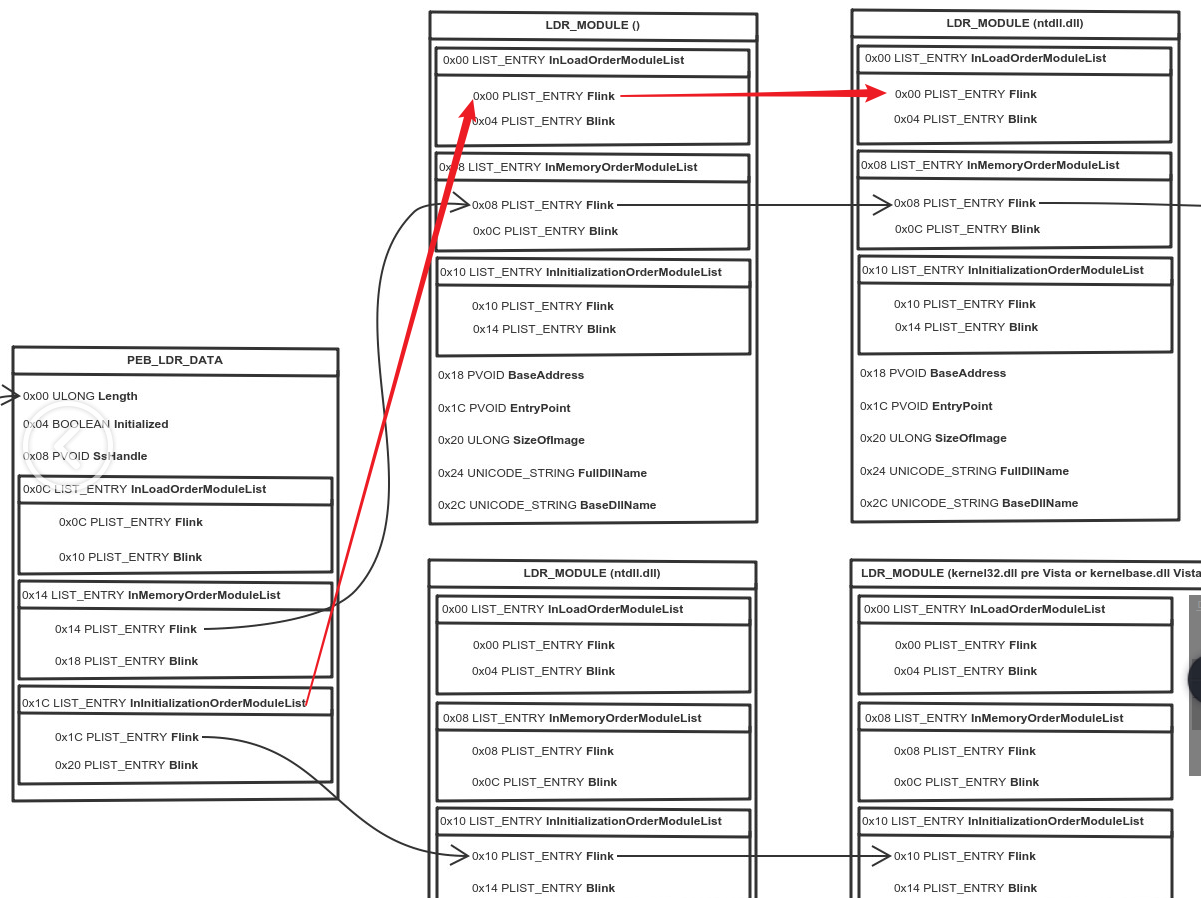
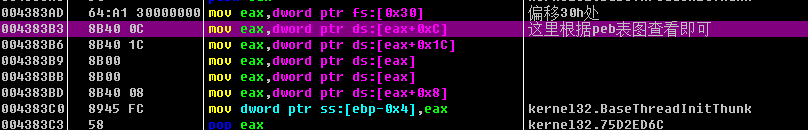
那么用dt \_PEB\_LDR\_DATA命令查看\_PEB\_LDR\_DATA结构体的结构，偏移1C指向哪里呢，可以看到指向了InInitializationOrderModuleList，这个成员是个\_LIST\_ENTRY结构体



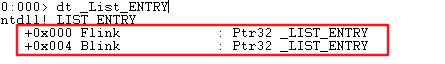


通过图看下PEB\_LDR\_DATA的成员，通俗来说就是有三个主要的LIST\_ENTRY：门。上面指向了第三个门也就是下图中的0x1c处的InInitializationOrderModuleList 

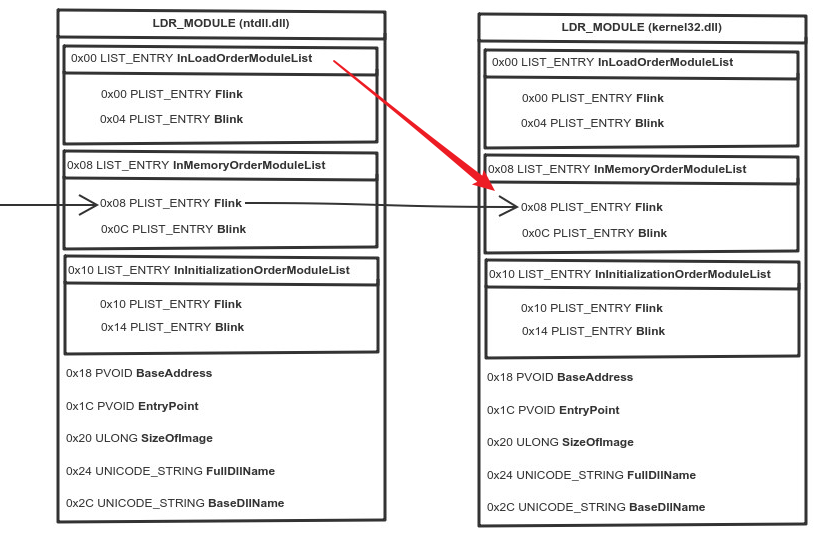
那么接下来的两次连续取0也就是



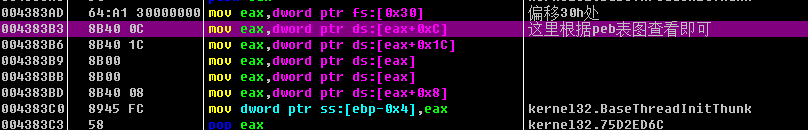
**用windbg查看：**



最后取到0x8

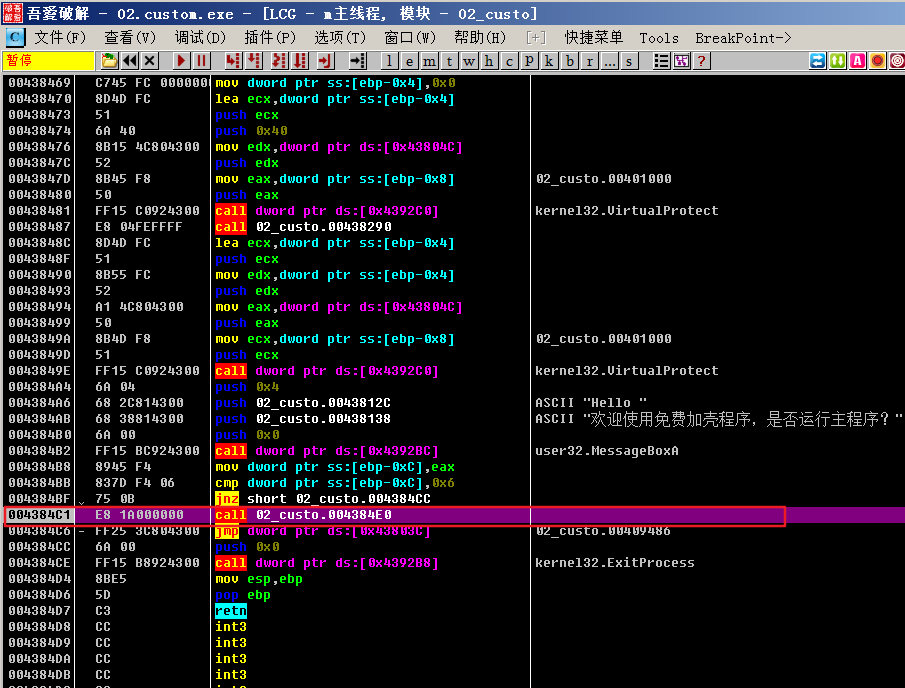


那么这样也就知道了这个壳确实是通过查找TEB结构来查找所有的导入函数的（参考编写遍历导入导出表时候的思路）

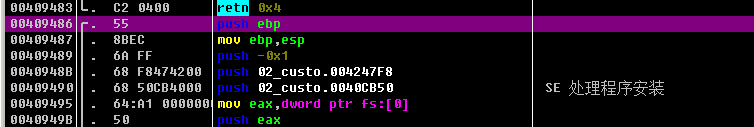


那么接下来壳要做的就是加密找到的IAT中的API（逐个加密API的地址即可），然后将加密的地址放到壳新申请的内存空间，而原来IAT中的地址就被填充为指向新申请的内存空间的地址，新的空间中除了加密的API地址，还有解密代码。这样当程序运行到原来IAT中的地址时，就会自动指向壳申请的空间，通过解密代码把加密的API地址还原，进行调用。

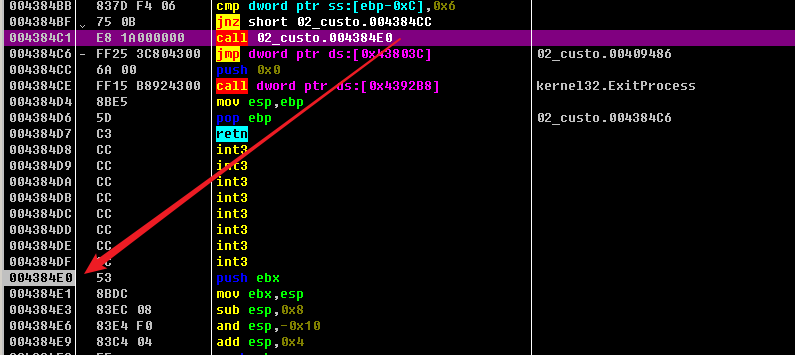
那么回到OD，当加壳程序框被用户确认后，才会执行申请空间和加密的逻辑，下面的jmp执行了一次大跳转，跳转到真正的OEP，因此jmp前的call成了最大的嫌疑者。



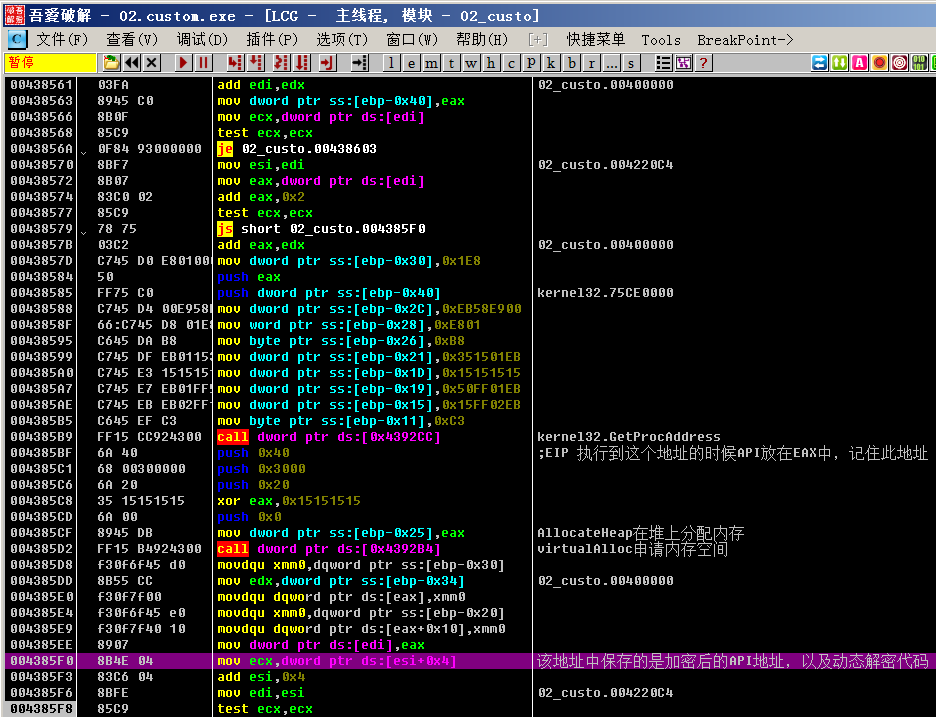
jmp过后可看到为真正的OEP，有的分析代码会看到提示



接下来分析call即可



记录如下的两个重要地址



**到现在一共三个地址：**

**OEP**：409486

**4385BF**：EIP执行到这里时，IAT刚刚被填充为申请的那段内存空间地址

**4385F0**：该地址中保存的是加密后的API的地址，以及动态的解析密码

通过代码解密：

// 初始化变量

// 临时变量，用来保存API地址

MOV dwEAX,0

// 当EIP执行到这个地址的时候API放在EAX中

MOV dwGetProcAddr,004385BF

// 当EIP执行到这个地址的时候IAT刚刚被填充为申请的那段内存地址

// 其地址中保存的是加密后的API地址，以及动态解密代码

MOV dwWriteIATAddr,004385F0

MOV dwOEPAddr,00409486 // IEP执行到OEP就可以dump了

// 清除所有软件断点

BC

// 清除所有硬件断点

BPHWCALL

// 设置硬件执行断点

BPHWS dwGetProcAddr,"x"

BPHWS dwWriteIATAddr,"x"

BPHWS dwOEPAddr,"x"

LOOP1:

RUN

CASE1:

CMP eip,dwGetProcAddr

JNE CASE2

MOV dwEAX,eax

JMP LOOP1

CASE2:

CMP eip,dwWriteIATAddr

JNE CASE3

MOV [edi],dwEAX

JMP LOOP1

CASE3:

CMP eip,dwOEPAddr

JNE LOOP1

MSG "到达OEP，可以dump了！！！"