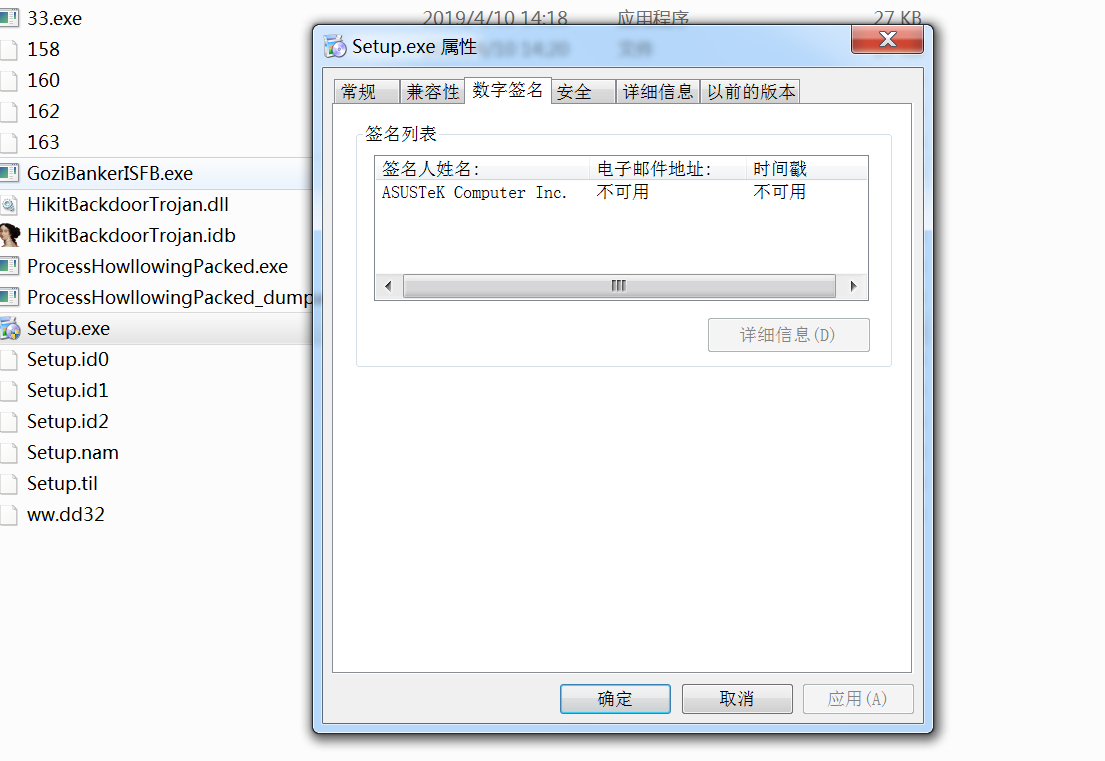
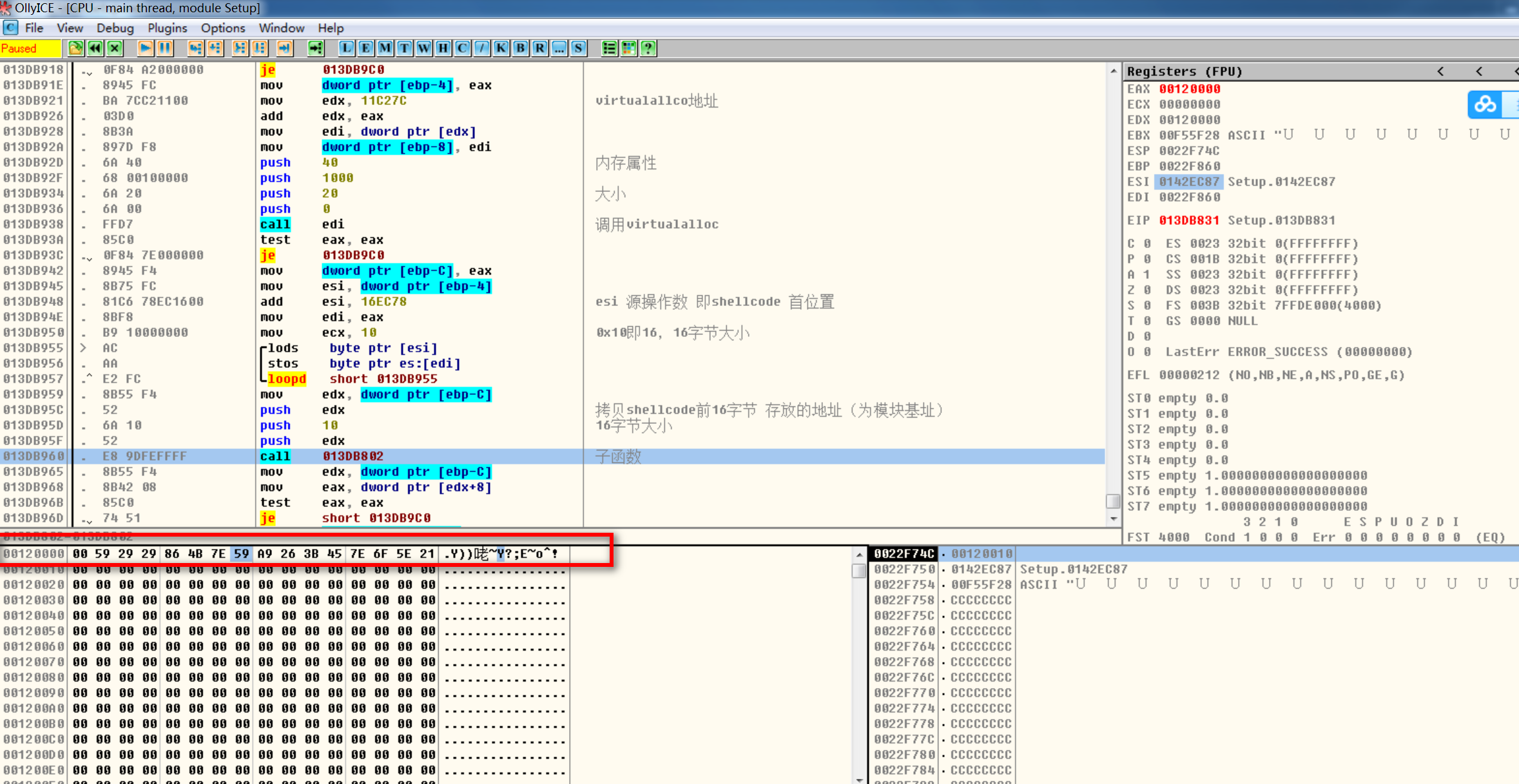
样本来源于<http://iec56w4ibovnb4wc.onion/Library/> ShadowHammer。

关于华硕供应链攻击和之前的cclear差不多,入侵之后窃取证书源码,替换源程序。

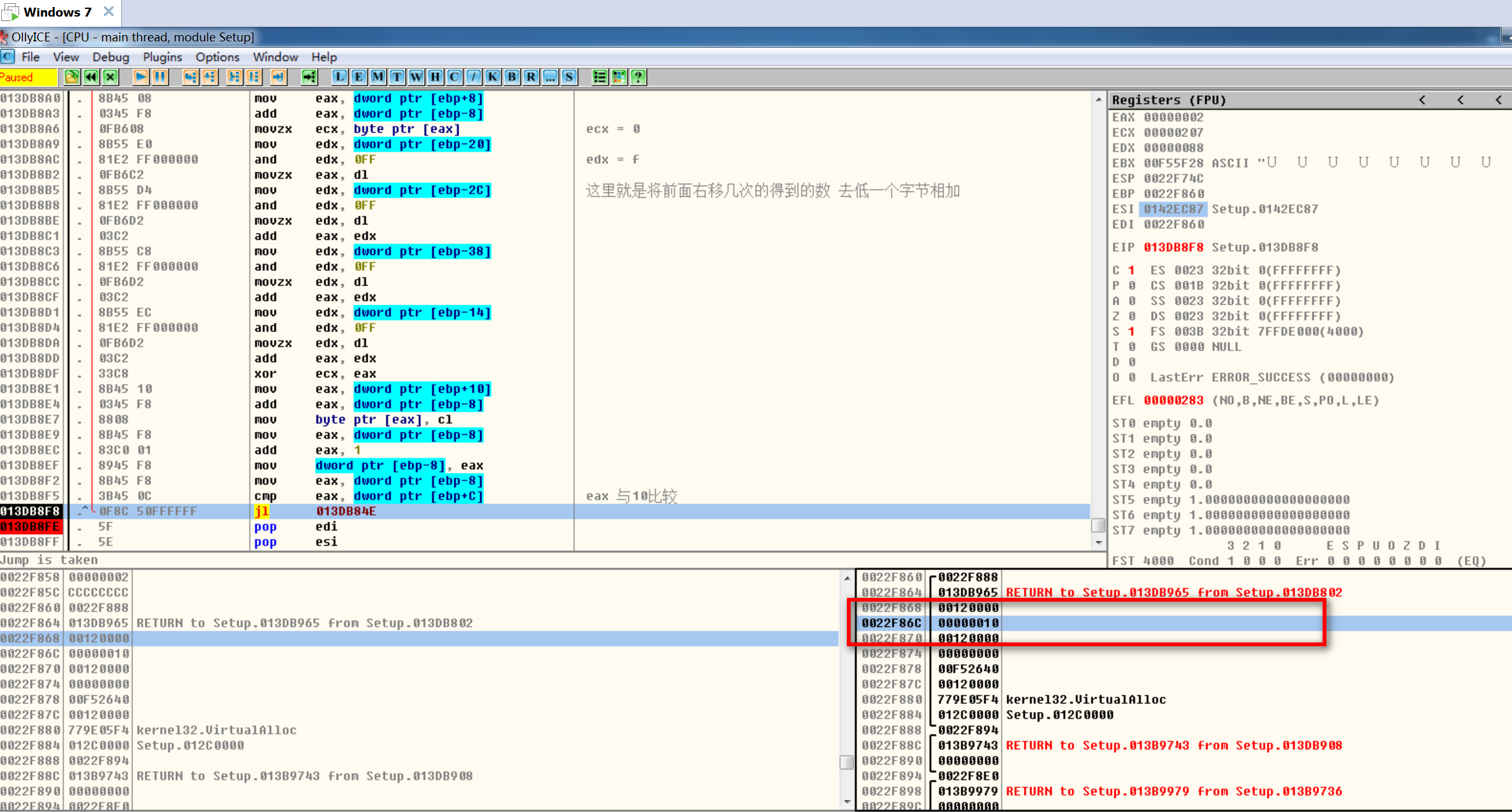


根据嘶吼的分析可知, 攻击者已经将Shellcode插入Setup.exe中，并修改代码，从而实现重定向执行。现在着重分析下shellcode解密与提取。

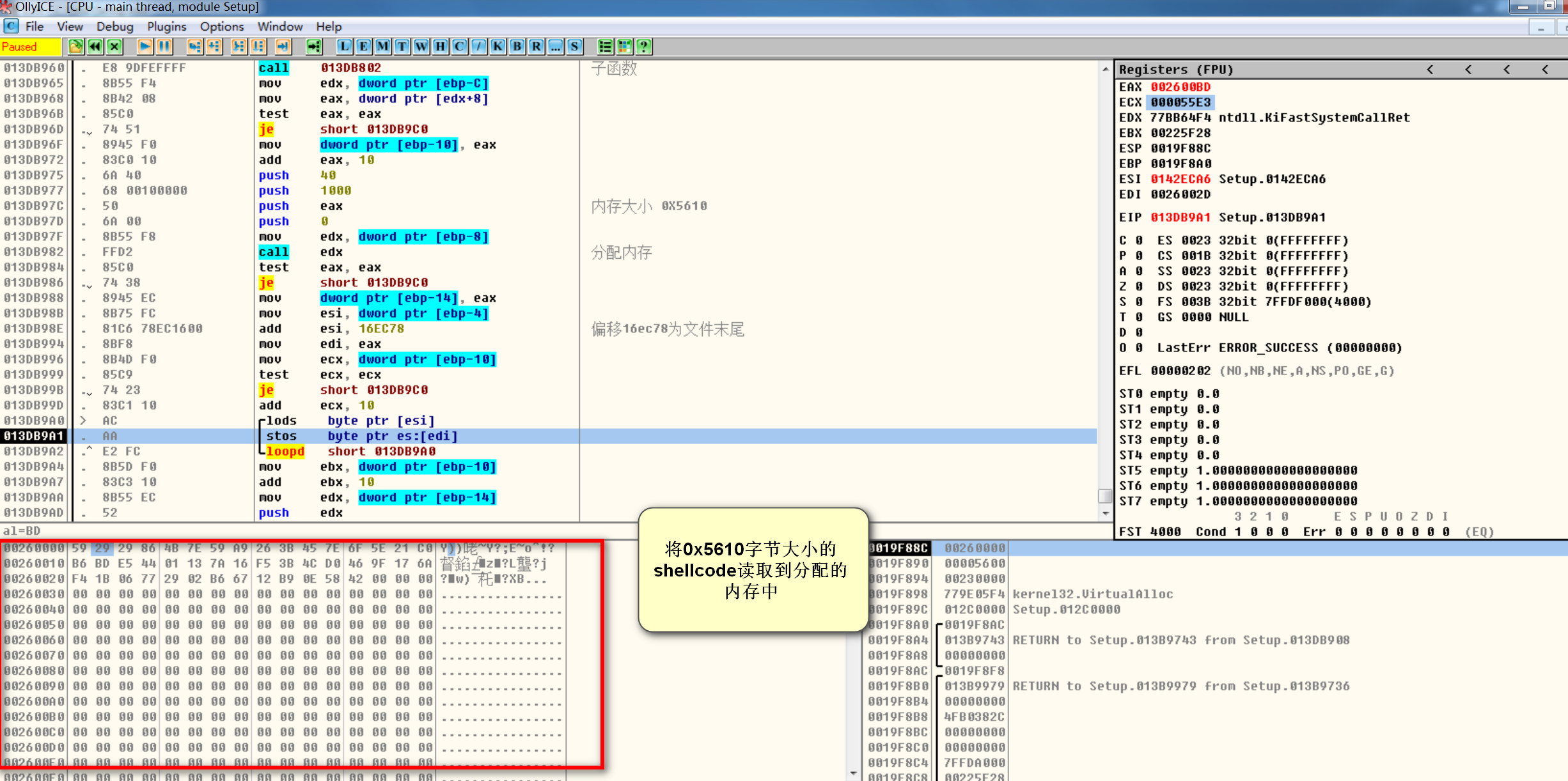
Ida中sub\_51B908函数为



拷贝shellcode前16字节到分配的内存中,在偏移1B802函数中对这16字节每一位进行移位操作,最后得到真正shellcode大小为0x5610字节



之后就是调用virtualalloc分配内存将shellcode加载到写入，



然后又一次调用偏移1B802处的函数对0x5610字节大小的shellcode每一个字节进程移位操作，最后执行shellcode入口偏移0FAB处.

