ctf.360.cn第二届，逆向部分writeup——第三题

转载

lyuharvey 于 2014-11-26 14:17:11 发布 97 收藏
原文链接：http://blog.51cto.com/cugou/1582765

题目：见附件

这题目是最快搞定的，提示很明确

> 这是一个被感染型病毒感染的可执行文件，试着修复该EXE程序，得到程序中的KEY

exe直接运行出错，OD打开后，发现入口点就是一个jmp

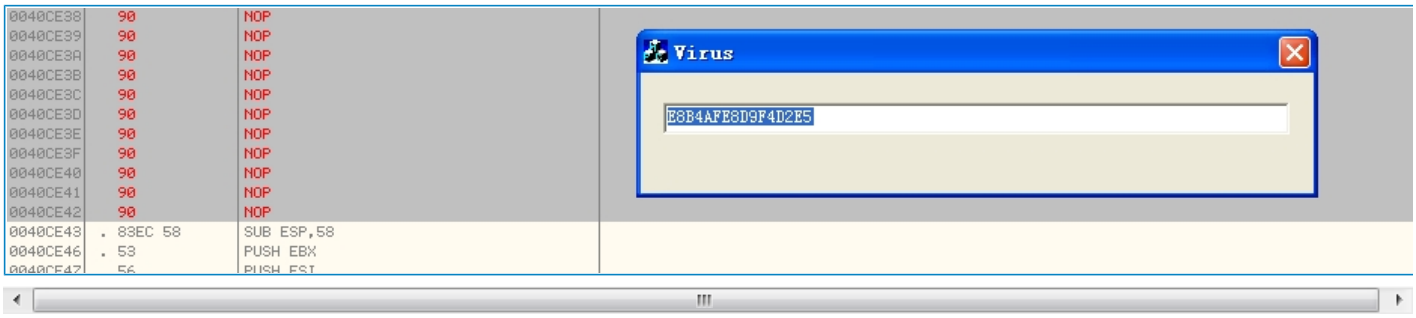
```
0040CE26  $ E9 D8110300   JMP Inject.0043E003
0040CE2B  . 68 48 2B 44 0 ASCII "hH+D",0
0040CE30  . 68 20 23 41 0 ASCII "h #A",0
0040CE35  . 64:A1 0000000 MOV EAX,DWORD PTR FS:[0]
0040CE3B  . 50            PUSH EAX
0040CE3C  . 64:8925 00000 MOV DWORD PTR FS:[0],ESP
0040CE43  . 83EC 58       SUB ESP,58
0040CE46  . 53            PUSH EBX
0040CE47  . 56            PUSH ESI
0040CE48  . 57            PUSH EDI
```

F8，跟踪到jmp后的地址，发现了程序运行出错的原因。

```
0043E003  > 8BC0          MOV EAX,EAX
0043E005  . 6A 00         PUSH 0
0043E007  . 68 5BE04300   PUSH Inject.0043E05B        ASCII "Key?NO!"
0043E00C  . 68 2BE04300   PUSH Inject.0043E02B        ASCII "A02B8DE7F2BCD4ED"
0043E011  . 6A 00         PUSH 0
0043E013    E8            DB E8
0043E014    F9            DB F9
```

实际上这个题目就是模拟病毒感染exe，修改文件入口指令，插入恶意代码的行为。

修补实际上就是找到真实的入口函数头的代码，将前面的jmp等指令nop掉。（修改OEP也行）



转载于:https://blog.51cto.com/cugou/1582765