文件：C:\test\ProcessHowllowingPacked.exe

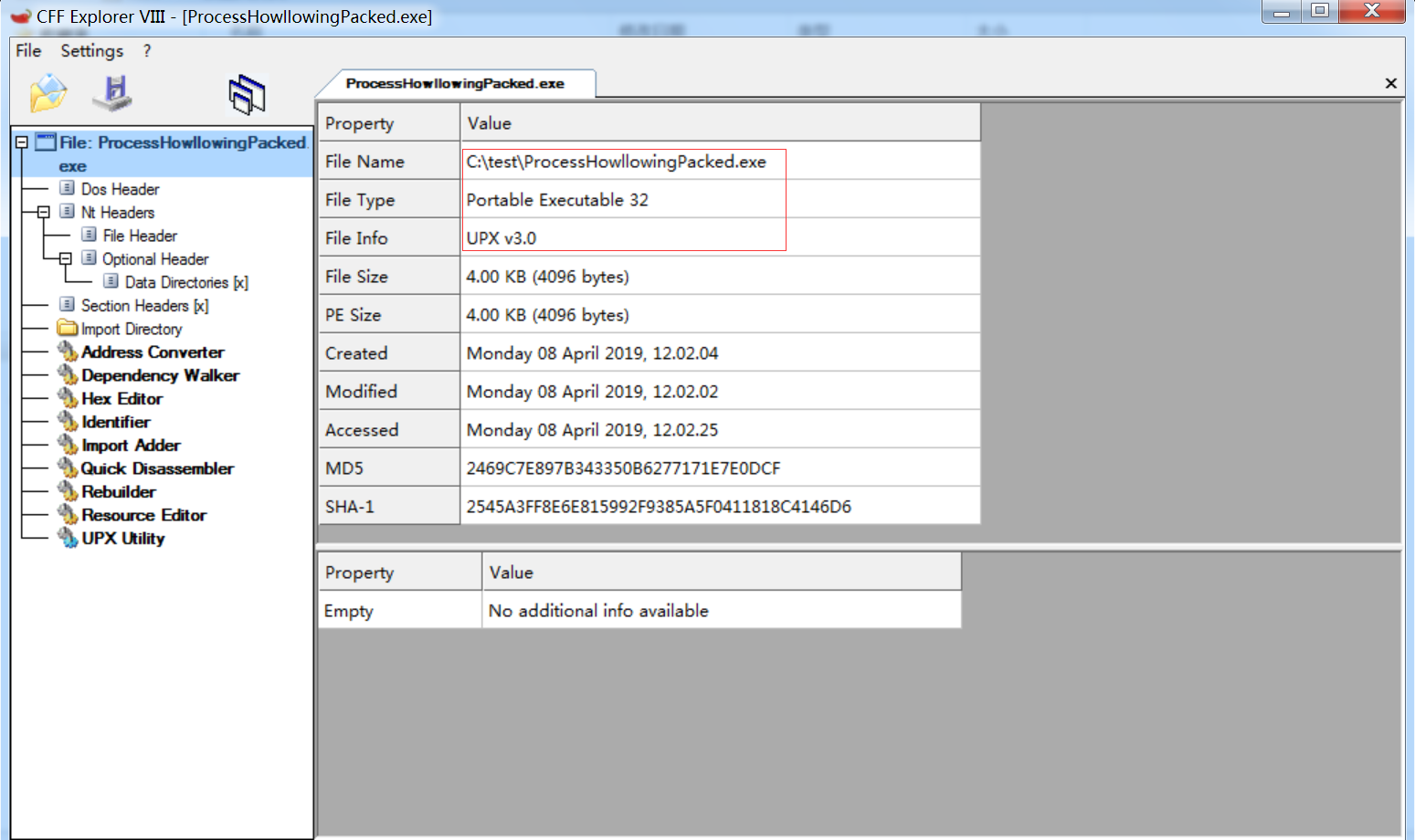
文件大小 4096字节

文件类型 PE32 executable (DLL) (console) Intel 80386, for MS Windows

MD5 2469C7E897B343350B6277171E7E0DCF

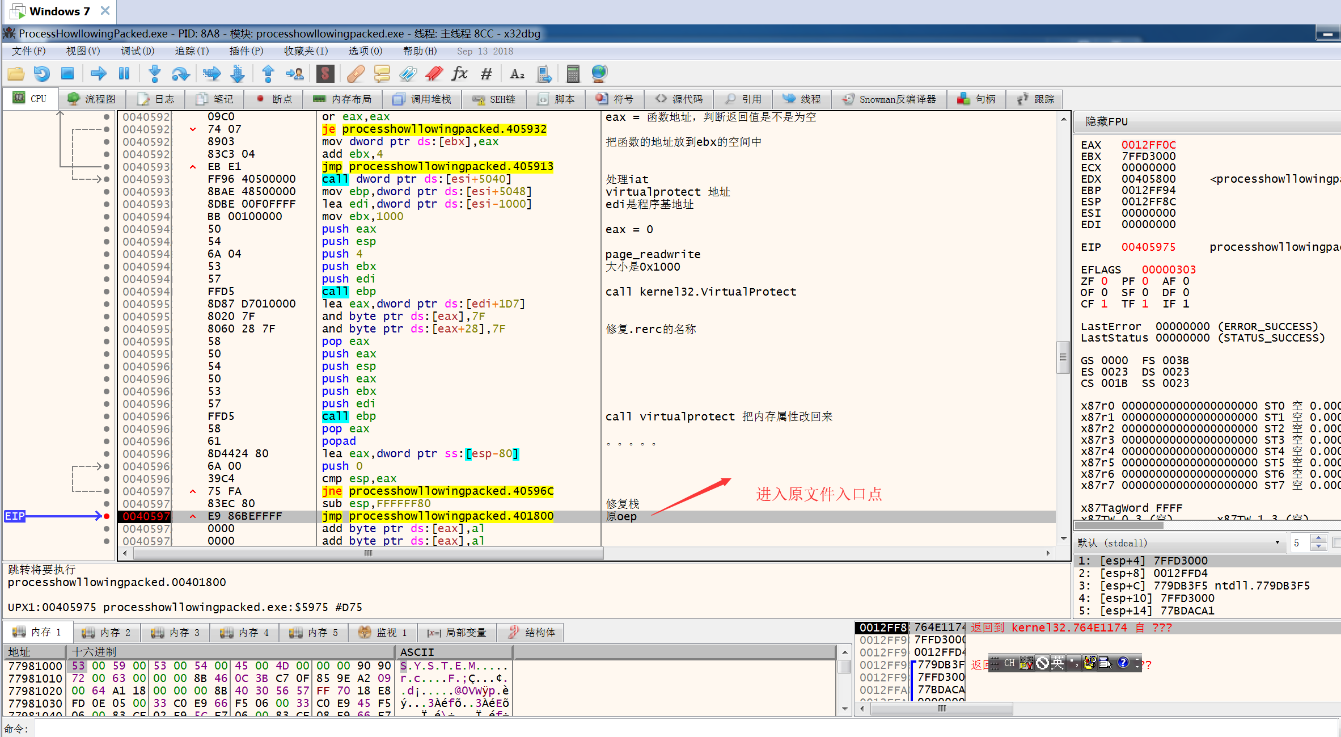
**查壳**

首先使用PEiD对样本进行查壳 以下是查壳结果

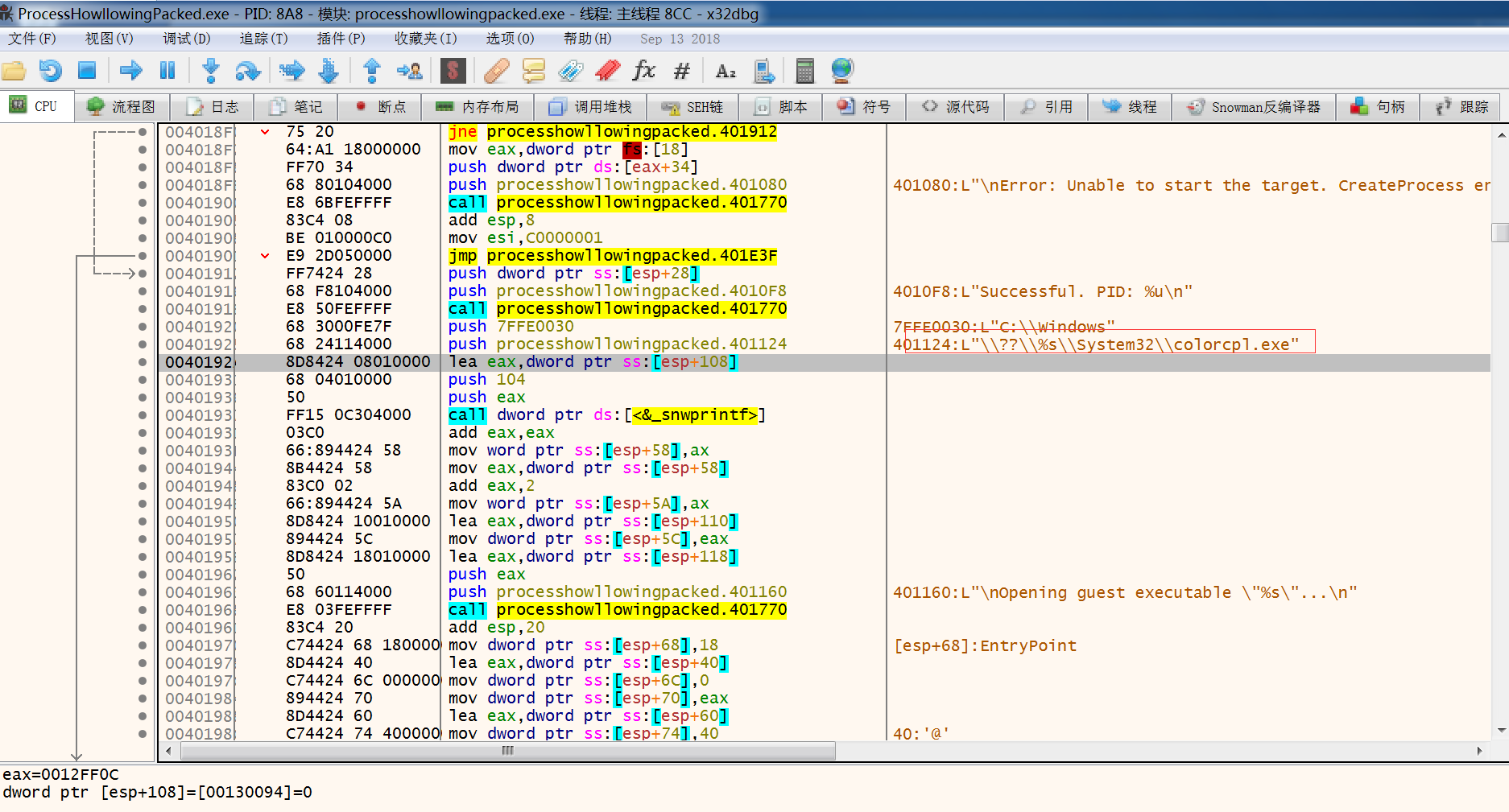


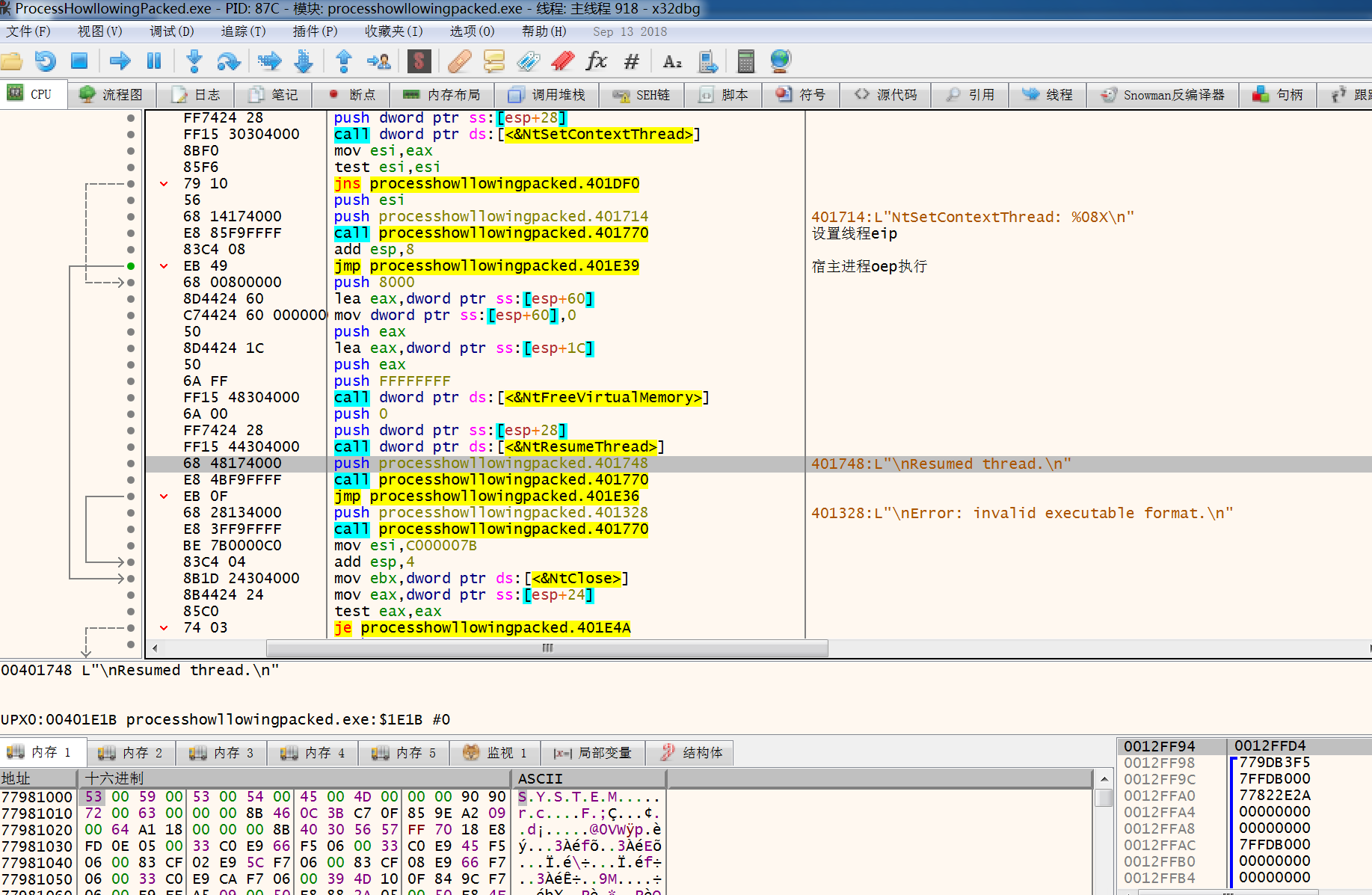
**结论：**病毒使用VC2015编写的 upx3.0的壳

加了壳什么都干不了先脱了再说，在进入原程序入口dump这时upx已经解压缩完成。



脱完壳修复iat后运行,可以看到创建挂起进程colorcpl.exe





最后设置线程eip为宿主进程oep,关闭原程序。

整个流程是这样的：

1、创建一个挂起的colorcpl.exe进程

2、找colorcpl.exe进程的OEP备用

3、在colorcpl.exe中开辟几块空间 存放自己的PeLoader、PE文件的ShellCode、参数结构

4、将PeLoader、ShellCode、参数结构写入colorcpl.exe中

5、Hook colorcpl.exe的OEP 改为PeLoader

6、恢复colorcpl.exe进程执行PeLoader加载ShellCode并运行

调用的winapi情况：

GetThreadContext获取进程Context,eax为进程入口点，ebx指向进程peb

ZwUnmapViewOfSection卸载colorcpl.exe进程内存空间数据

VirtualAlloc分配内存空间

WriteProcessMemory将代码写入到分配的内存

SetThreadContext设置挂起进程状态

ResumeThread唤醒进程运行