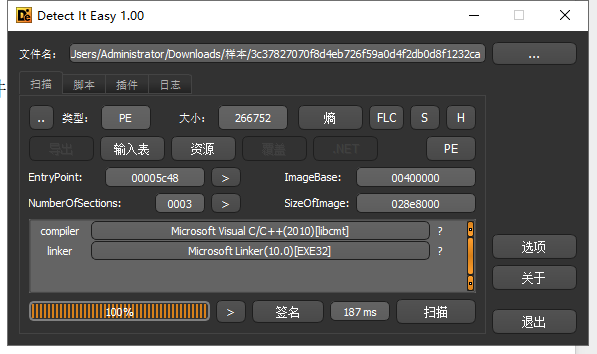
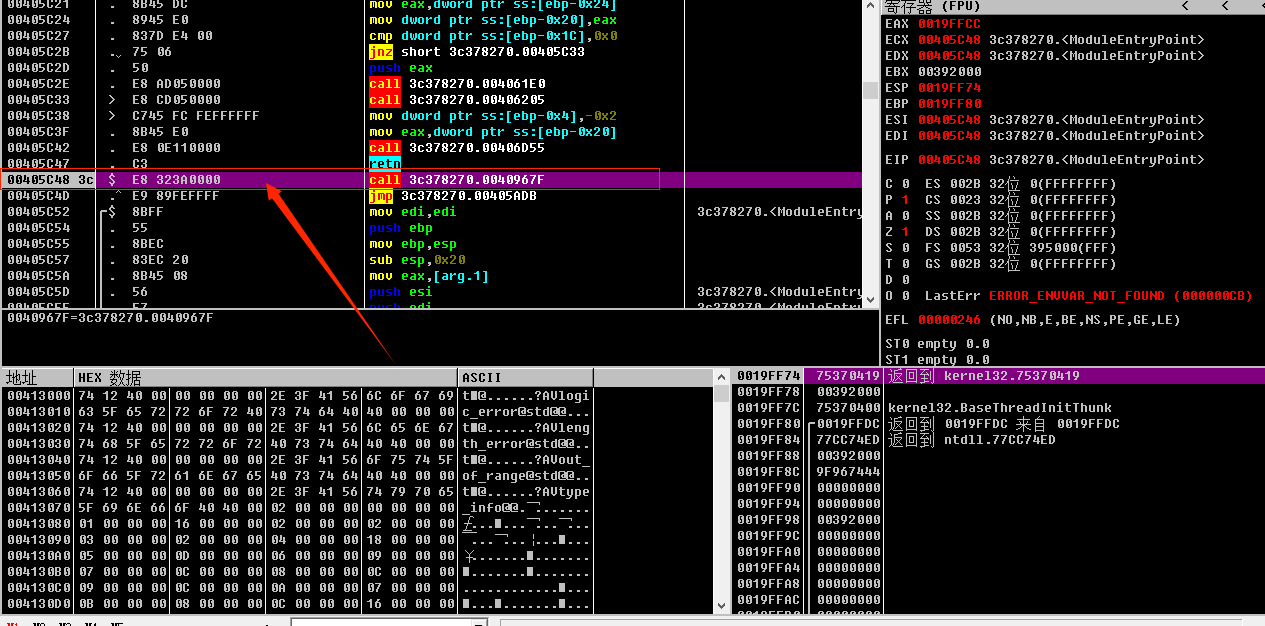
# 某恶意软件分析学习

## 一、分析过程如下

通过DIE判断为加壳，开发语言为c/c++



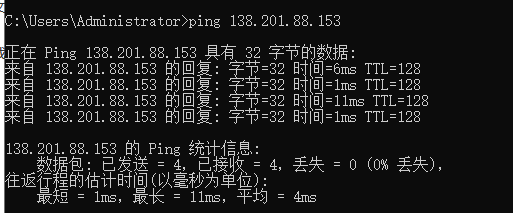
程序入口点5c48,使用编辑器为vs编辑器



## 行为分析



发现有一个恶意连接ip为138的ip地址



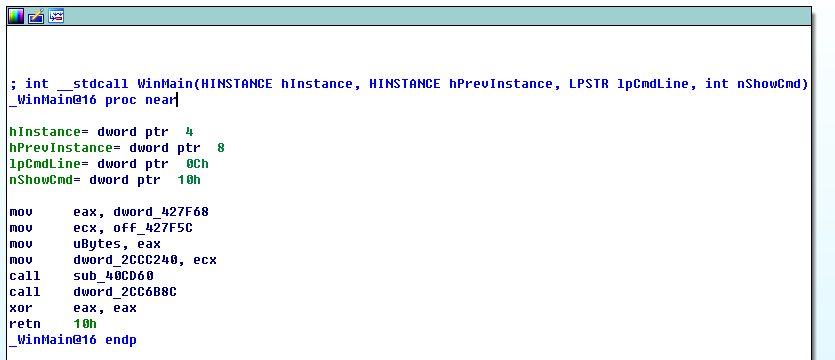




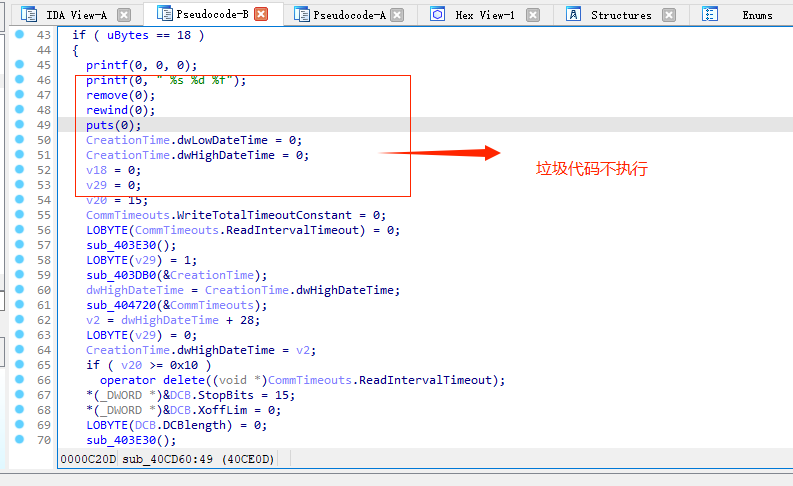


## 详细分析（静态+动态）

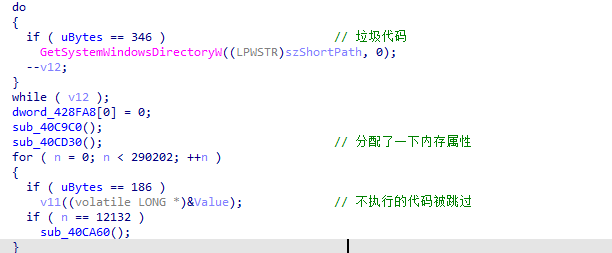
1. 首先跟进主函数winmain



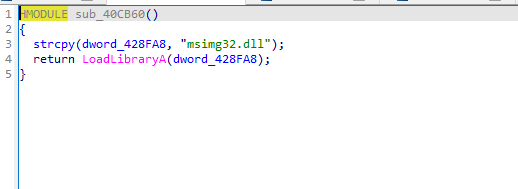
跟进40CD60







动态加载msing32.dll



### 总结

这是一个远控类型的病毒，截至到目前，该c2地址仍然在使用状态，具有监控屏幕，操作文件等功能