

**恶意代码课程实验报告**

**实验九**

****

学 院 网络空间安全学院

专 业 信息安全、法学

学 号 2111454

姓 名 李潇逸

班 级 信息安全、法学

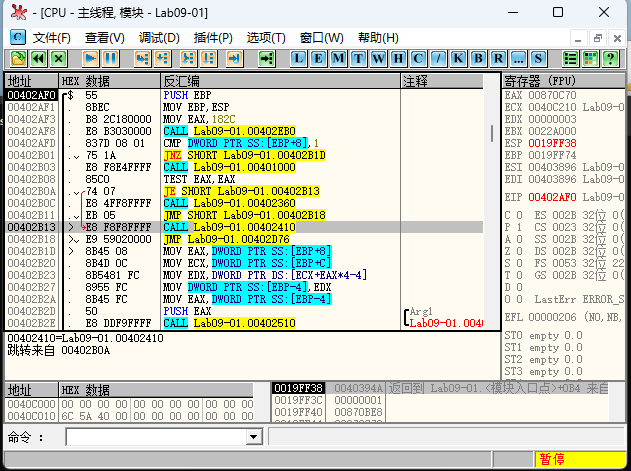
1. **实验环境**

VMWARE，Windows11

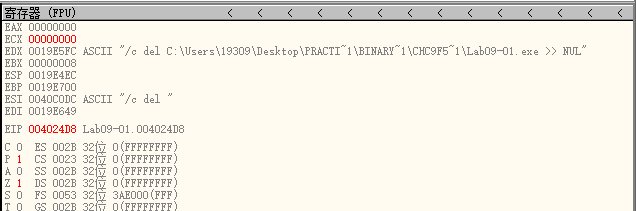
1. **实验工具**

IDA，YARA，OllyDBG

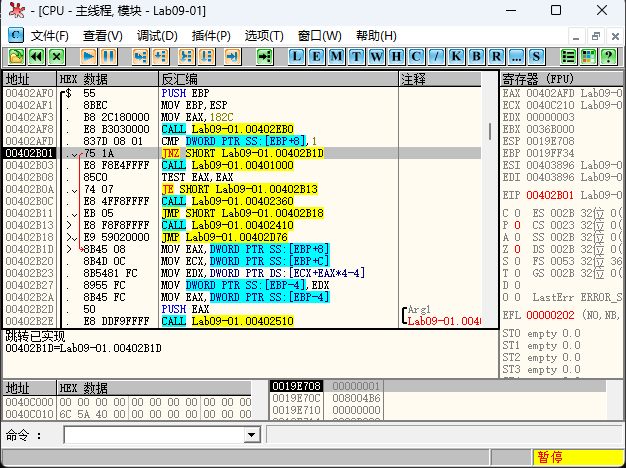
1. **实验过程**
2. **Lab09-01**
3. **启动ollydbg，开始进行调试。找到main函数调用点并进入可得到如下界面：**



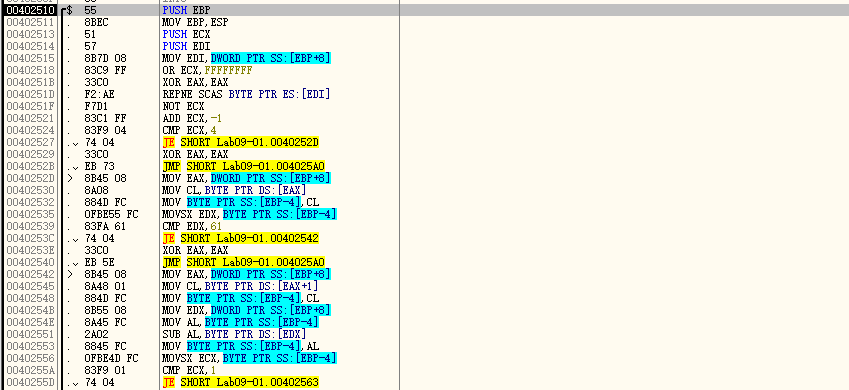
**在402AFD进行了一个比较，查看命令行参数与1进行比较，之后跳转到401000继续进行程序运行；之后由于查找不到相应的注册表，因此调用402410处的代码。在这里我们发现，程序构造了一个字符串，法分析发现该字符串目的是将自身删除。**



**为了使恶意代码可以正常运行，将尝试一些操作。首先就是尝试在命令行中添加参数，从而跳过402AFD处的字符串比较。我们添加了-in作为输入，然而并没有什么作用。继续分析可以认为命令行中仍需要输入一个密码进行下载**



1. **在本程序中存在4个命令行命令。-in下载服务，-re删除程序，-c更新配置，-cc打印配置。**
2. **我们发现对于本程序来说，判断口令是否正确主要取决于以下函数：**

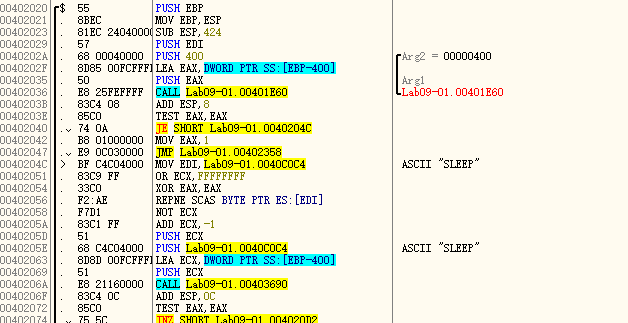


**在本函数中我们发现，是否进行程序取决于最后的返回值。因此我们就要在这里进行修改，让其返回值永远为真，即可做到不输入密码。具体而言需要插入**

**MOV EAX,0x1;**

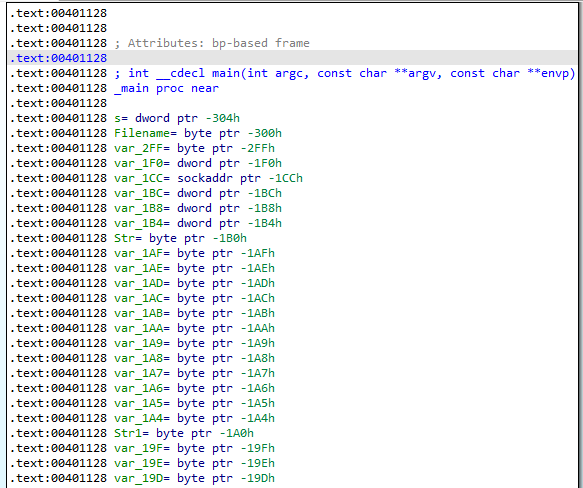
**RETN;**

1. **HKLM\SOFTWARE\Microsoft \XPS\Configuration**
2. **分析发现，从如图所示的部分开始可以发现相应操作：**

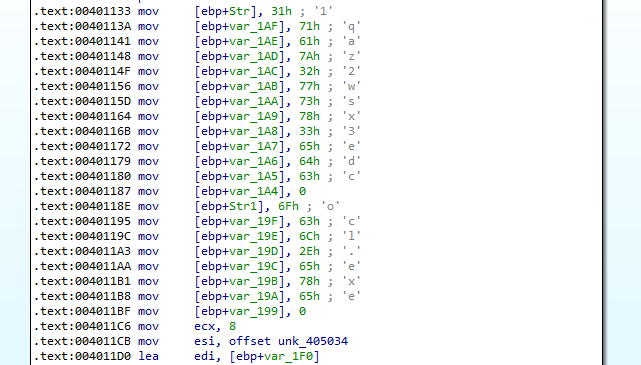


**当传入字符串为SLEEP时，恶意代码开始执行睡眠；当传入字符串为UPLOAD时，通过相应端口链接远程服务器，读取数据并在本地创建文件夹；当传入字符串为DOWNLOAD时，读取本地文件并进行传输；当传入字符串为CMD时运行命令行；当传入字符串为NOTHING时，不进行任何操作。**

1. **有的，会向http://www.practicalmalwareanalysis.com发送一些请求**
2. **Lab09-02**
3. **可以发现可被理解的字符串大部分为导入函数和cmd**
4. **看似是直接结束**
5. **打开ida pro，发现该程序的主函数部分从401128开始**

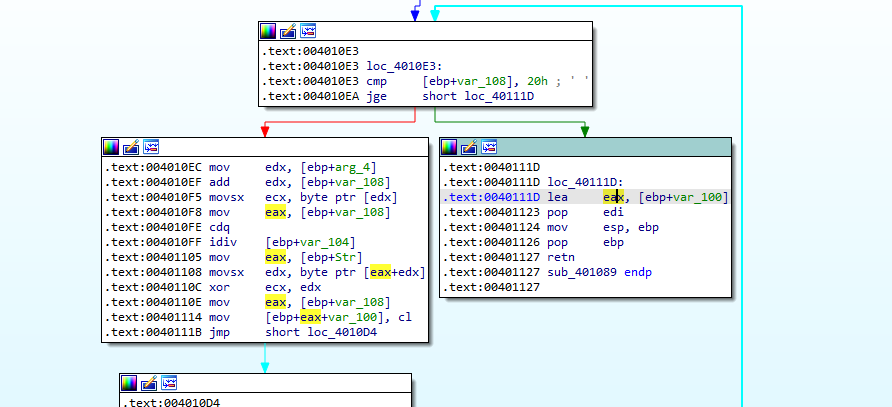


**之后使用ollydbg进行调试，可以发现该程序创建了两个字符串：1qaz2wsx3edc和ocl.exe**

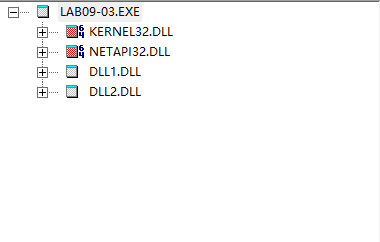


**接下来在这一部分可以发现有一个字符串比较，分析发现当文件名与ocl.exe不相符时则程序不会运行。因此将本文件重新命名为ocl.exe后就可以进行运行。**

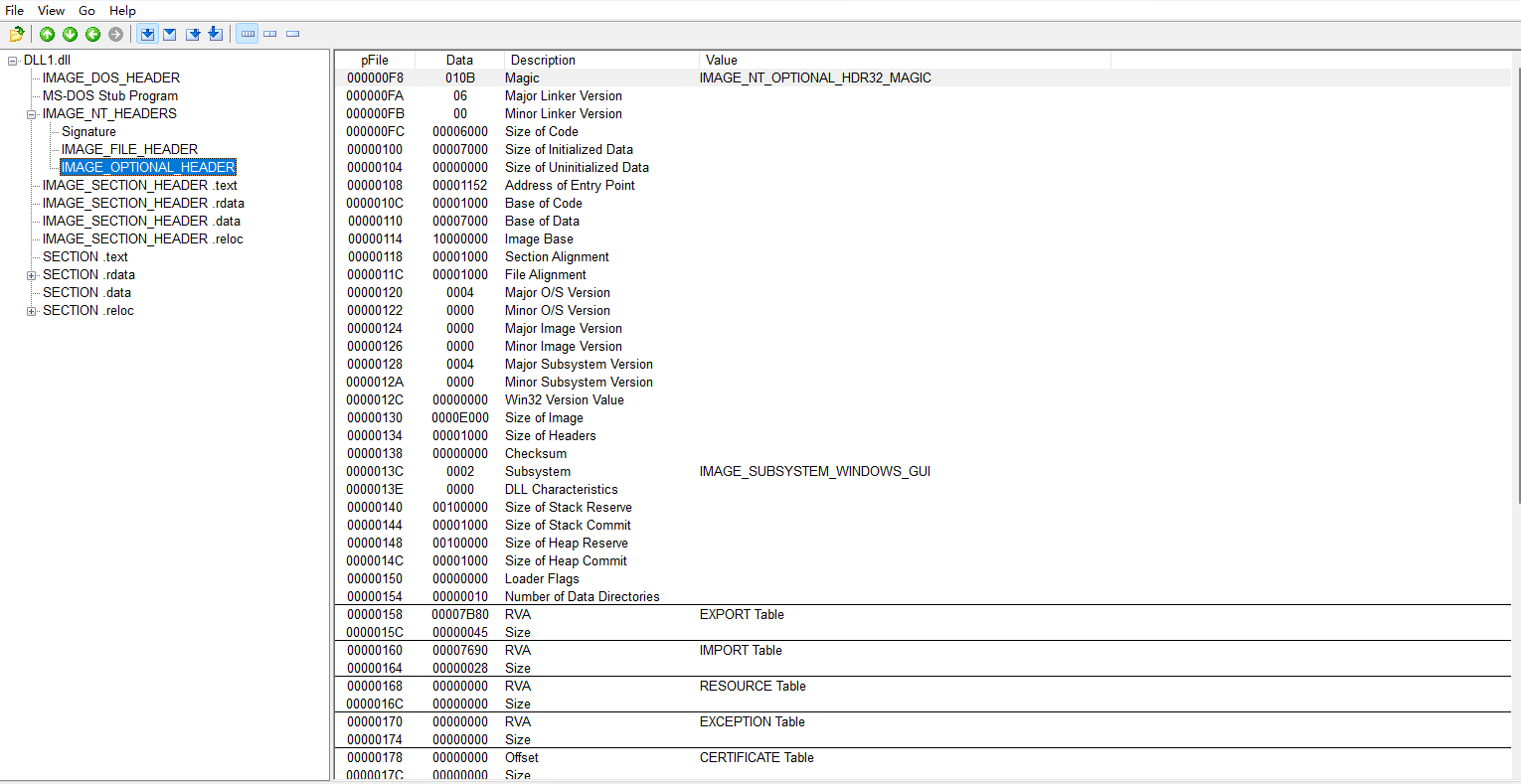
1. **综上所言，在栈上创建了一个字符串，用与进行混淆**
2. **将文件名改为ocl.exe，同时设置断点，运行程序后发现传入了两个参数：第一个是输入的密文字符串，第二个是1qaz2wsx3edc的字符串。**
3. **在这里发现了www.practicalmalwareanalysis.com**

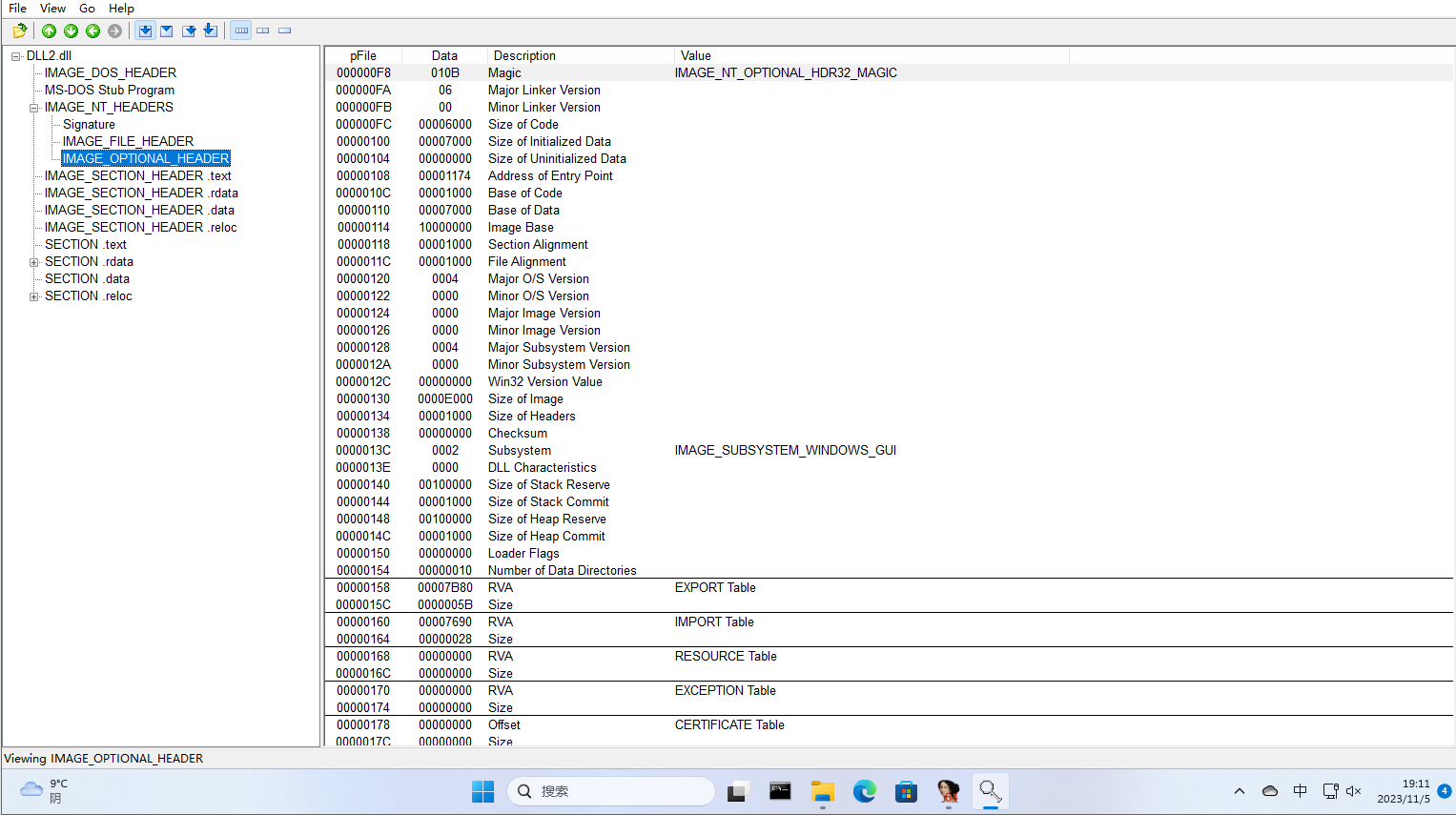
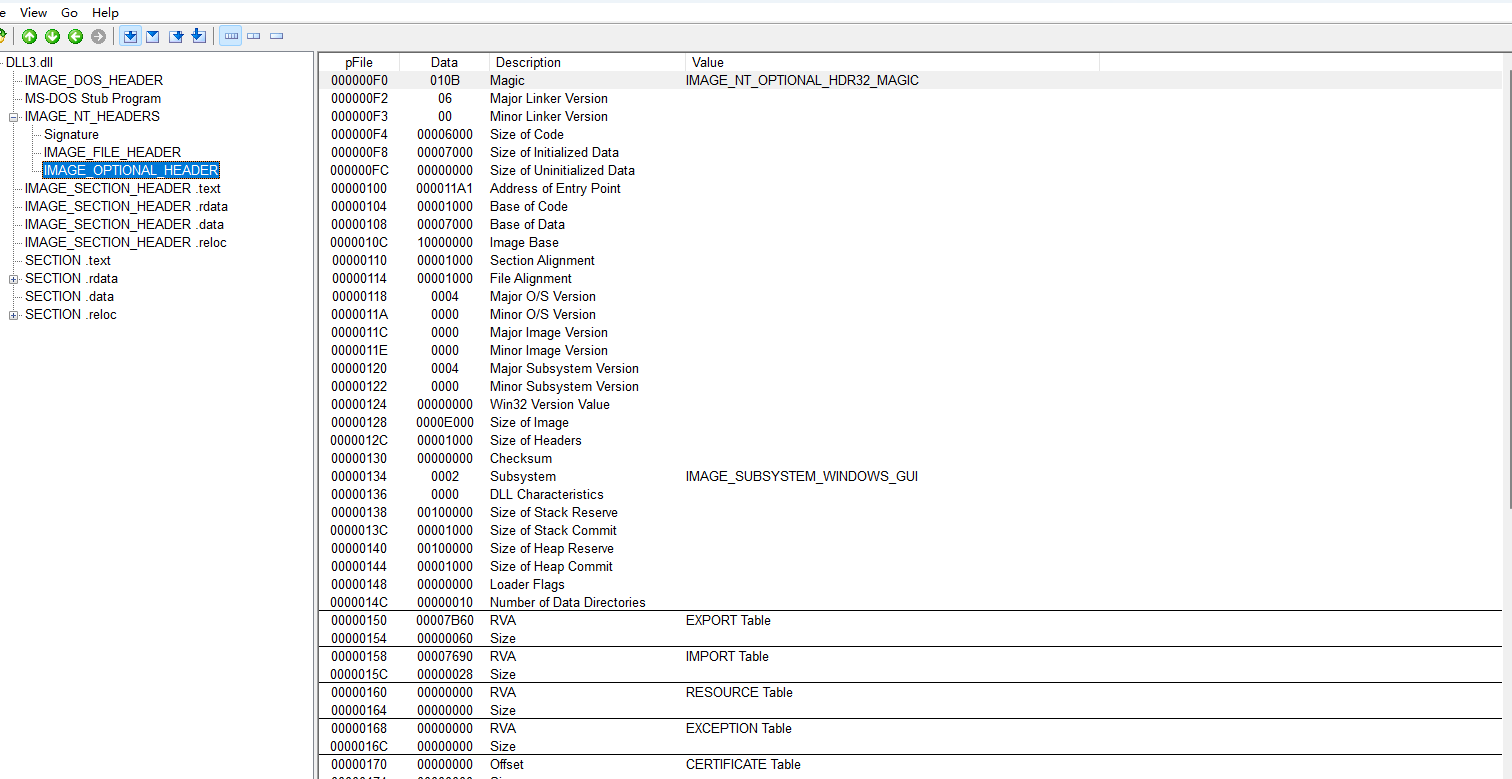
****

1. **使用1qaz2wsx3edc进行异或混淆**
2. **绑定一个套接字后进行反向shell命令**
3. **Lab09-03**
4. **查看导入表发现导入了KERNEL32.DLL、NETAPI32.DLL、DLL1.DLL、DLL2.DLL**

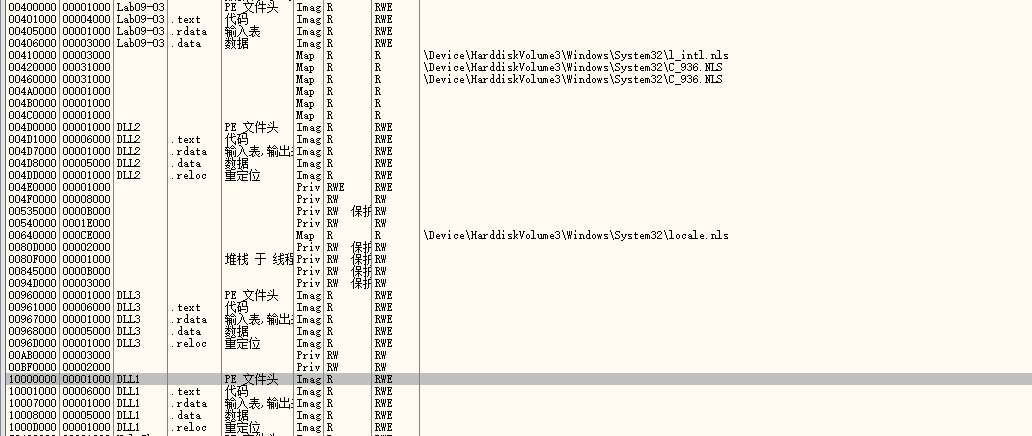


1. **都是0x10000000**



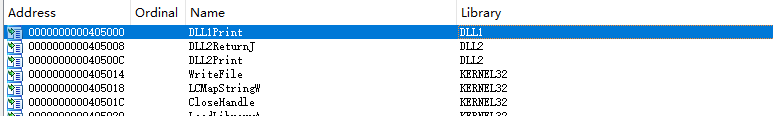


1. **打开程序，在导入dll文件后设置断点，运行后打开内存如下：**

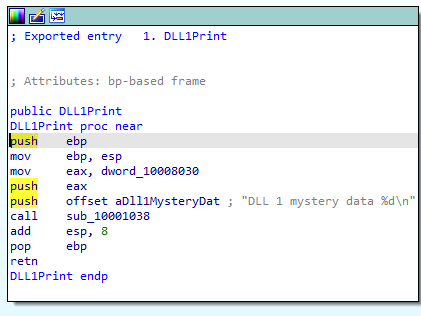


**发现dll1地址0x10000000，dll2地址0x004D0000，dll3地址0x00400000**

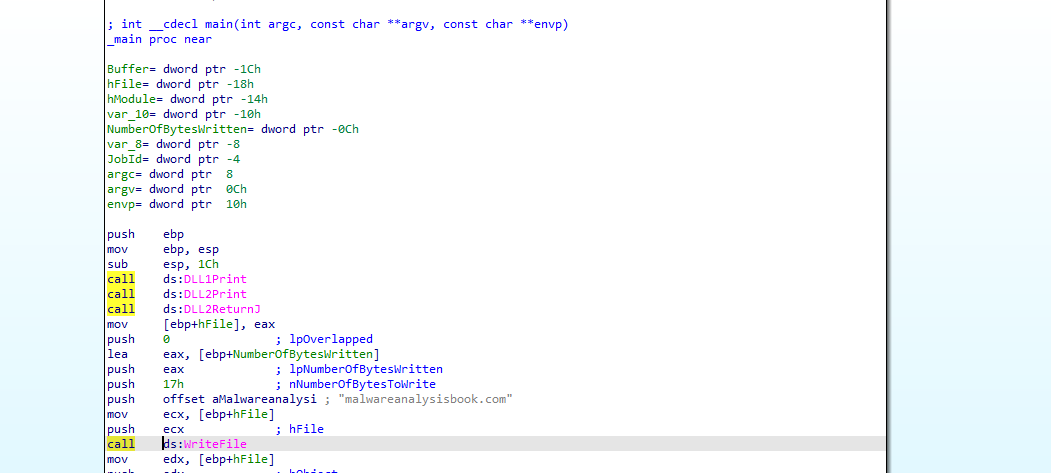
1. **查看导入表，发现导入了dll1print函数**



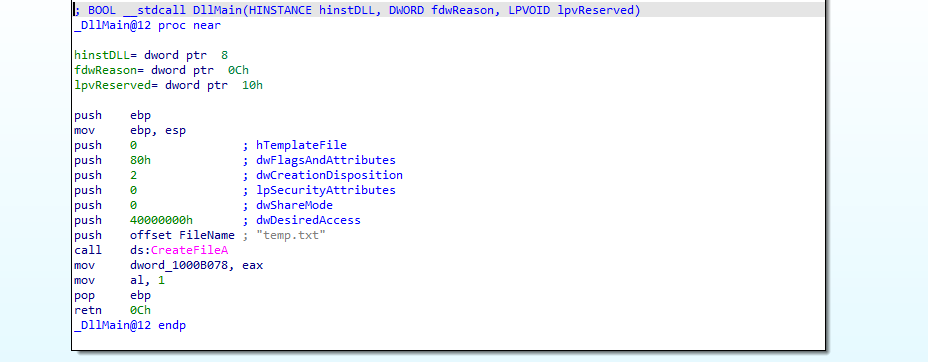
**反汇编后发现要输出DLL 1 mystery data %d\n**



1. **调用的地方如下：**



向上发现dllreturnj，反汇编发现返回了一个字符串temp.txt，可以认为将此作为文件名



1. **在此处发现相关函数**



**向上查看可知参数从Dll3GetStructure得到**

1. **分析相应部分得出，第一组神秘数据是进程ID，第二组神秘数据是temp.txt文件句柄，第三组神秘数据是ping [www.malwareanalysisbook.com的位置](http://www.malwareanalysisbook.com的位置)**
2. **手动加载并输入**
3. **实验心得**

**初步学习了如何使用工具进行恶意代码分析，对恶意代码和恶意代码分析工具有了更深的理解。**