

**恶意代码课程实验报告**

**实验七**

****

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

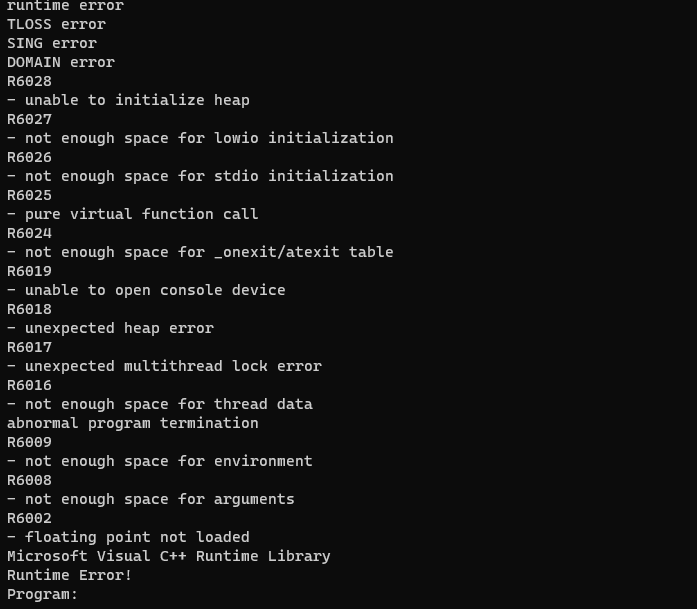
1. **实验环境**

VMWARE，Windows11

1. **实验工具**

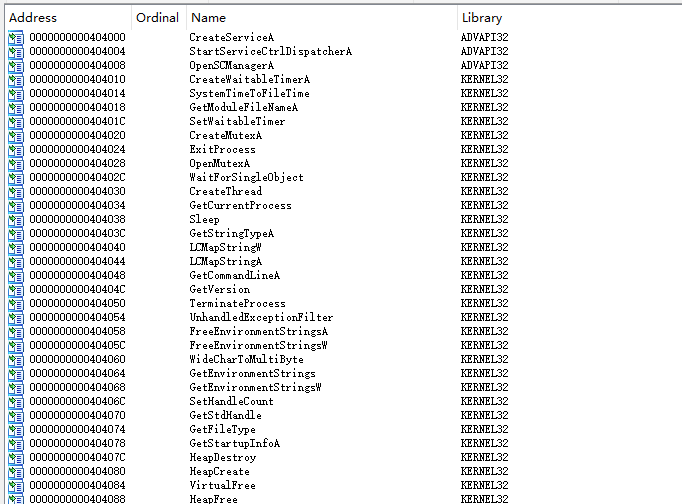
IDA，YARA

1. **实验过程**
2. **Lab07-01**
3. **首先使用静态分析技术。Strings发现了如下有意思的字符串：**

屏幕截图 2023-10-29 132036

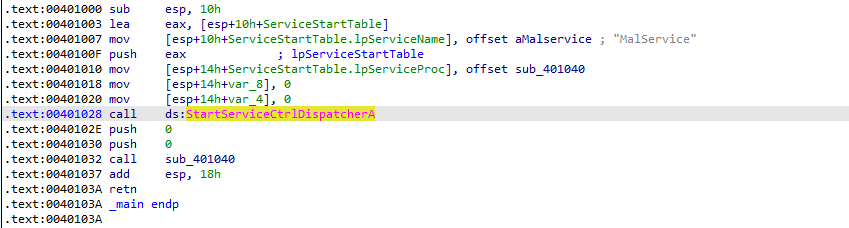
**可以认为本程序要进行网络链接并尝试链接一个网址。**

**打开IDA后开始检查本程序的导入表**

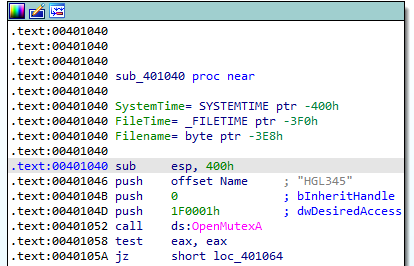


**在这里我们发现了CreateServiceA以及OpenSCManagerA，正是这两个函数想要创建一个服务，以保证系统重启后依旧可以运行。**

1. **我们进入主函数部分**

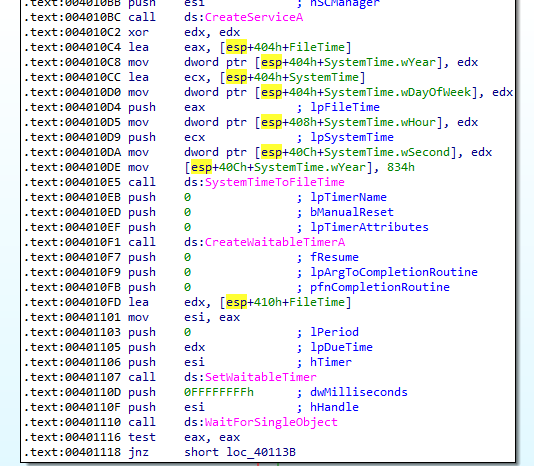


**首先调用了StartServiceCtrlDispatcherA，之后立即使用sub\_401040处的函数**

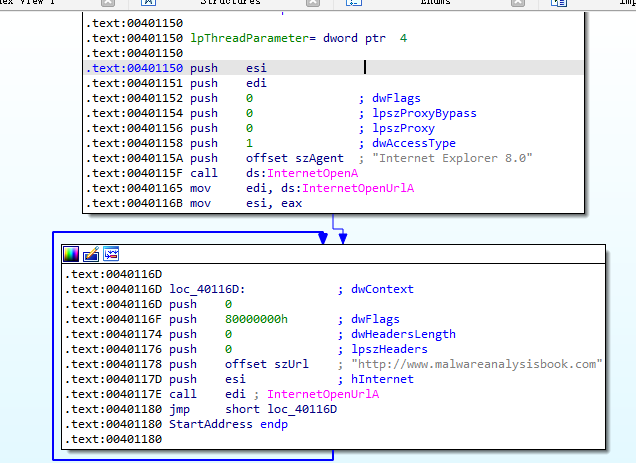


**它使用了OpenMutexA，试图获取HGL345这样的一个句柄，获取成功则退出程序。该互斥量作用是保证同时只有一个该程序处于运行状态**

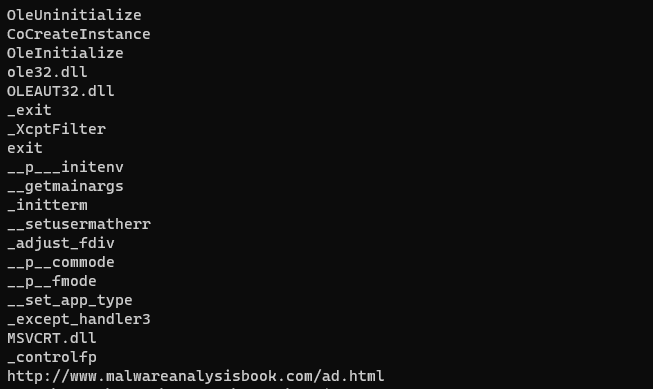
1. **HGL345句柄和Malserve服务**
2. **在下列代码中我们可以发现本程序开始设置一系列有关于时间的内容**



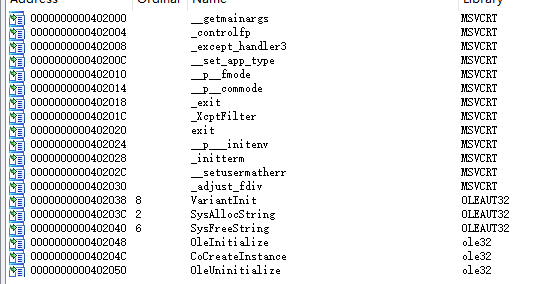
**在时间的部分设置为了2100年1月1日，之后调用SystemTimeToFileTime转换时间格式。之后程序开始等待，开始执行时发现了Internet Explorer 8.0和http://www.malwareanalysisbook.com可以作为网络特征**



1. **如上文所述，本程序将等待到2100年1月1日并向http://www.malwareanalysisbook.com发送请求，看起来是DDOS攻击**
2. **2100年1月1日开始后不会停止**
3. **Lab07-02**
4. **首先静态分析，发现了一个网址非常有意思**

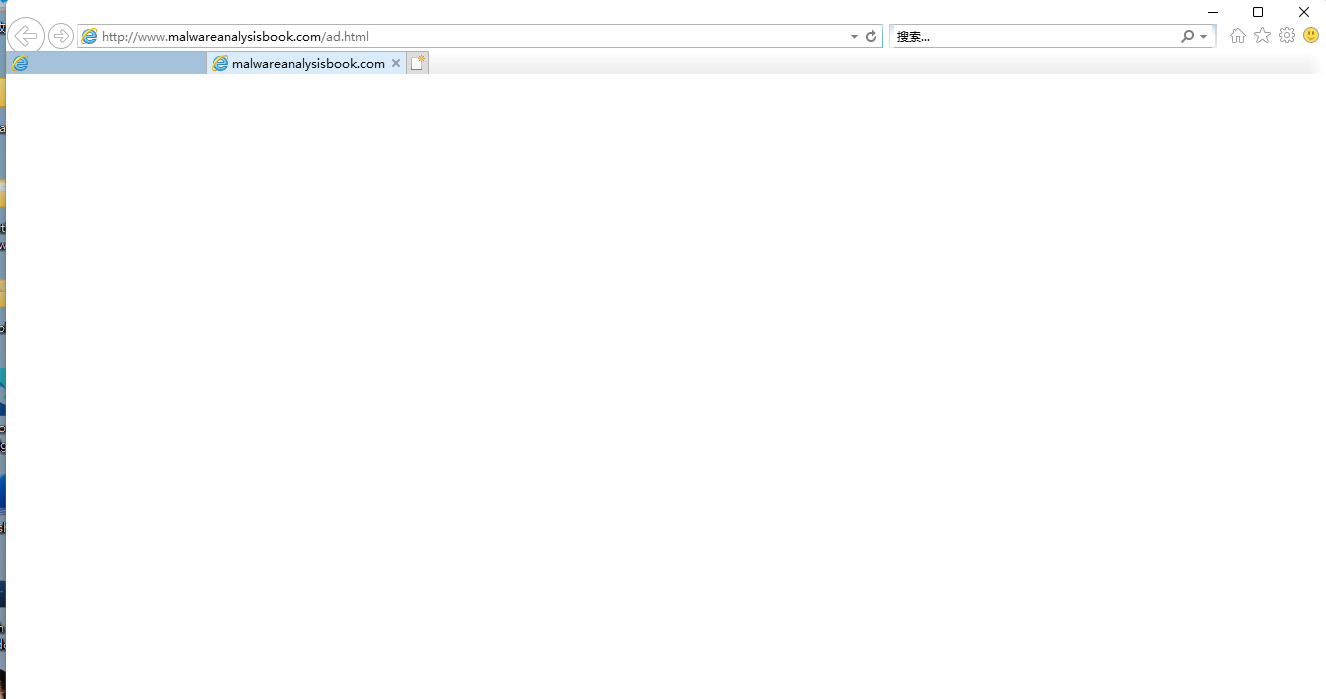


**之后查看该程序的导入表如下**

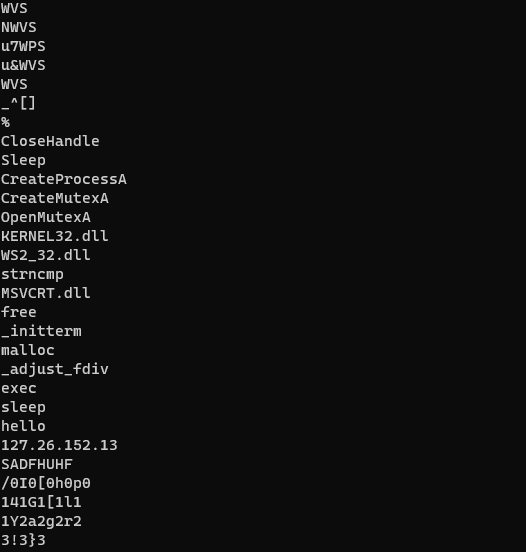


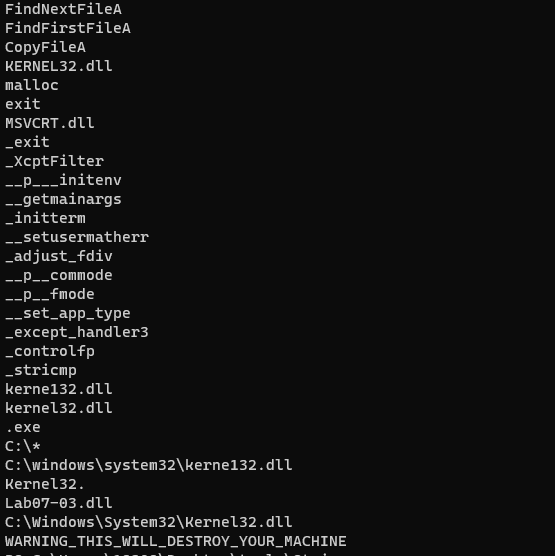
**发现所有函数都与COM相关，动态分析后发现该程序将打开一个网页，不存在持久化驻留的迹象。**

1. **运行后向用户展示广告页面，由于版本原因，现在已无法看见具体显示**

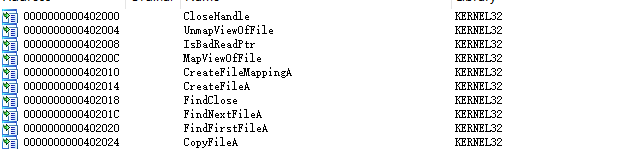


1. **显示广告后完成执行**
2. **Lab07-03**
3. **首先执行静态分析，发现了dll和exe程序中的一些有意思的字符串**

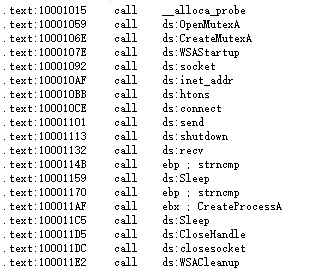




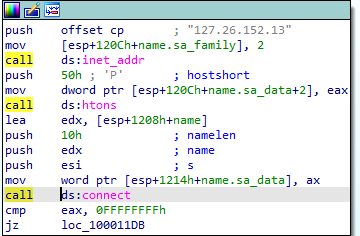
**接下来我们查看了exe文件的导入表，这些函数告诉我们该程序可能会创建一个文件并写入内存之中。**



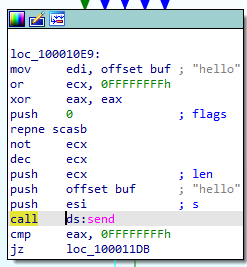
**接下来查看dll程序中的call函数。发现了socket函数，需要传输一些数据。**



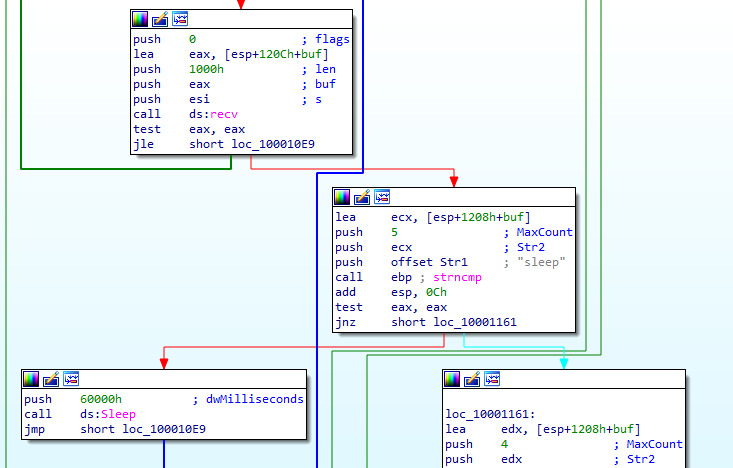
**发现在connect之前会确定IP地址和端口号**



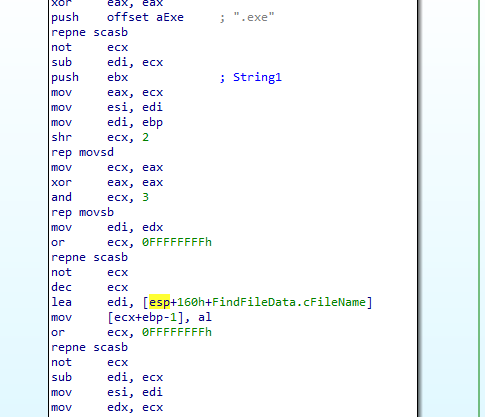
**发现其要发送到受害机器的内容是Buf中的内容**



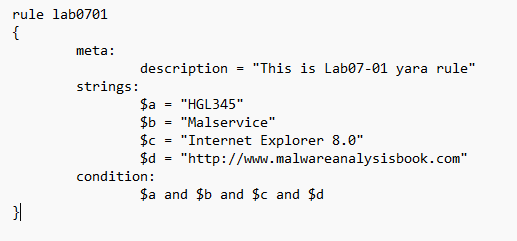
**接下来开始接受一些东西，分析发现是接受一个sleep字符，若接收到这样的字符就开始执行sleep操作**



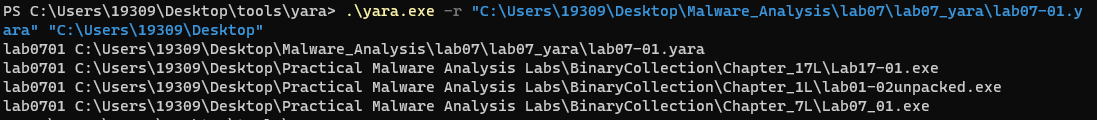
**在分析exe文件时发现，该程序将会对所有导入他的exe程序进行修改，从而保持长久的驻留**



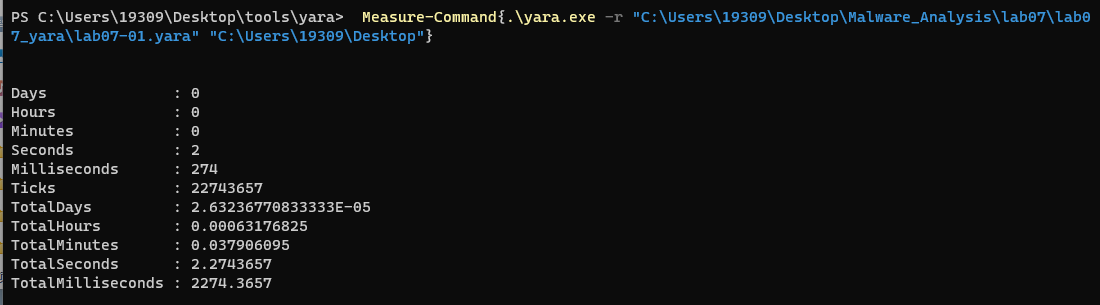
1. **kerne123.dll**
2. **我们可以认为此程序要留下一个难以删除的后门，之后连接一个远程服务器，同时后门有两个功能，一个是执行命令，另一个是执行睡眠。**
3. **难以移除。这是由于他感染了计算机上的所有exe文件。**
4. **Yara练习**
5. **Lab07-01**



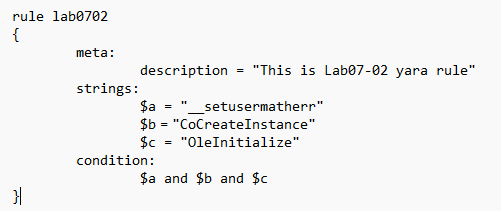
**运行后发现可成功抓取相应的恶意代码**



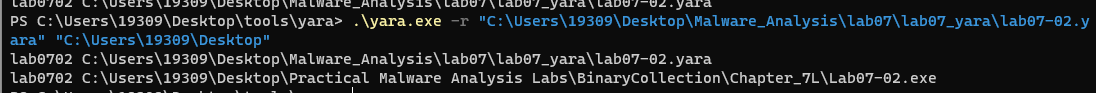
**共执行了2274.3657ms**



1. **Lab07-02**



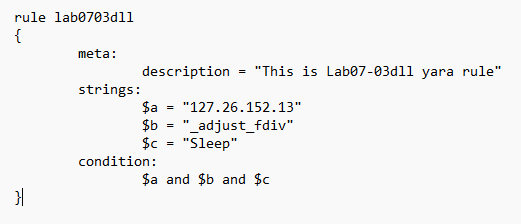
**运行后发现可成功抓取相应的恶意代码**



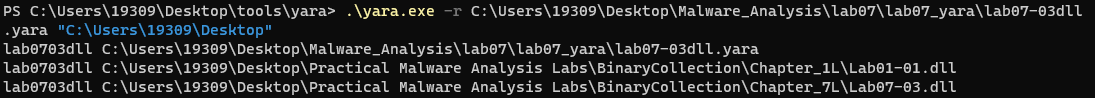
**共执行了2057.1643ms**



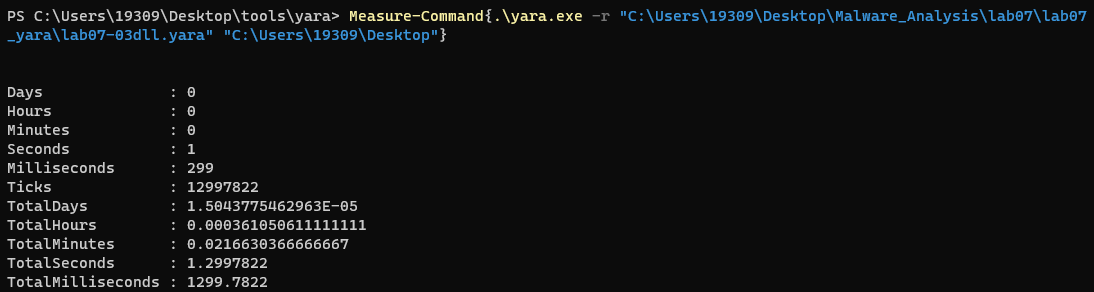
1. **Lab07-03**



**运行后发现可成功抓取相应的恶意代码**



**共执行了1299.7822ms**



1. **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。**