

**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

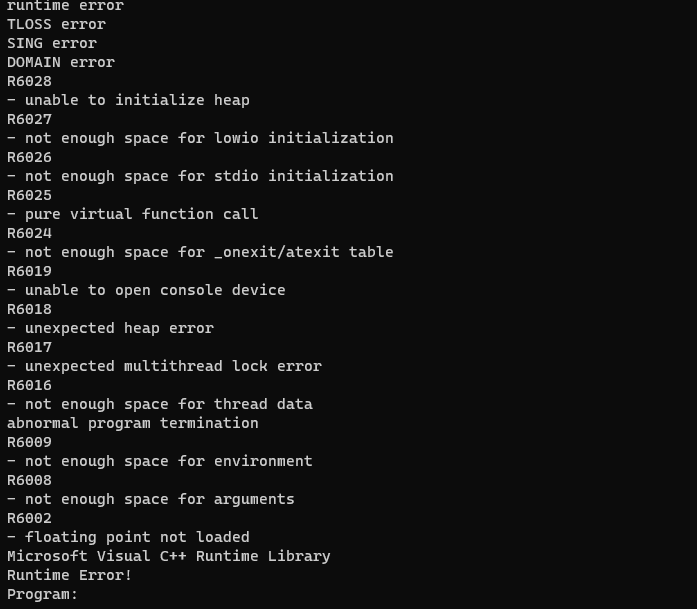
1. **实验环境**

VMWARE，Windows11

1. **实验工具**

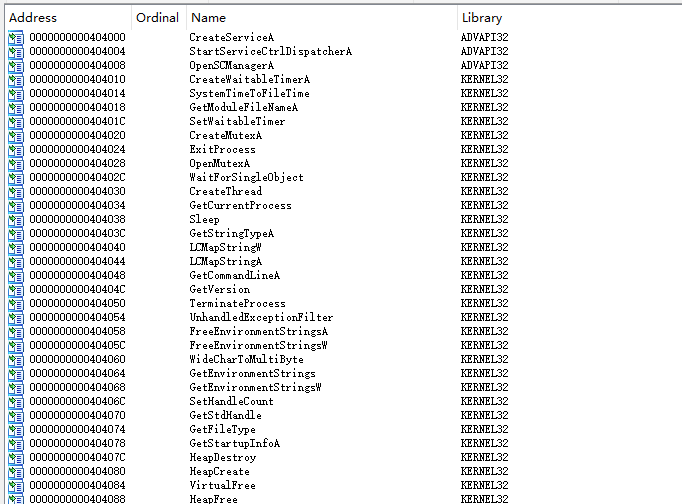
IDA，YARA

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

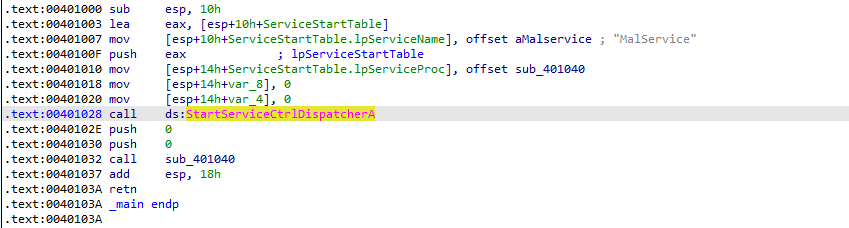
**可以认为本程序要进行网络链接并尝试链接一个网址。**

**打开IDA后开始检查本程序的导入表**

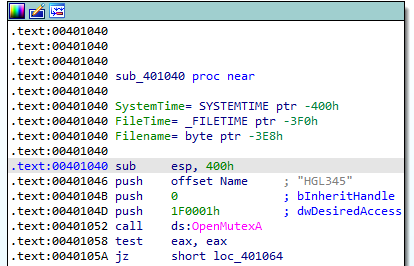


**在这里我们发现了CreateServiceA以及OpenSCManagerA，正是这两个函数想要创建一个服务，以保证系统重启后依旧可以运行。**

1. **我们进入主函数部分**

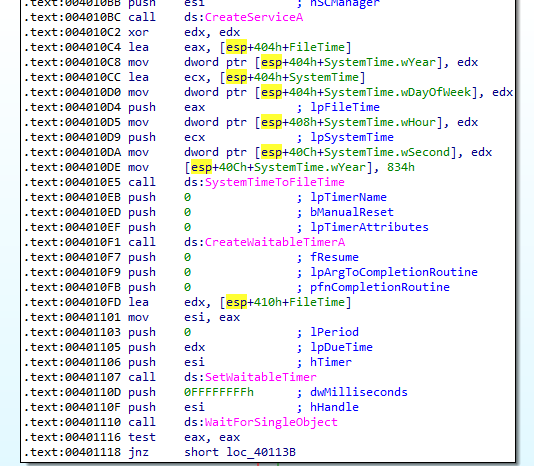


**首先调用了StartServiceCtrlDispatcherA，之后立即使用sub\_401040处的函数**

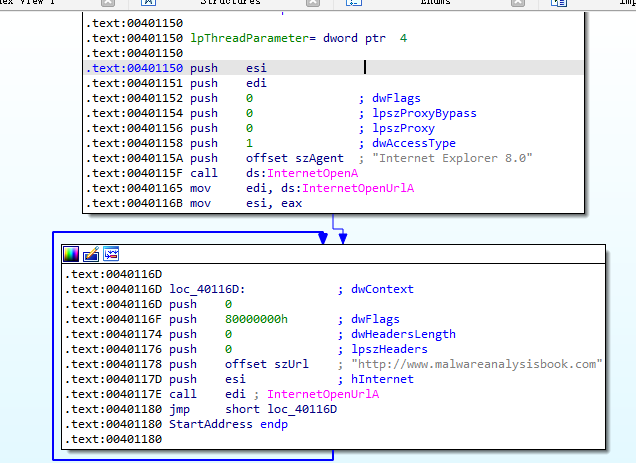


**它使用了OpenMutexA，试图获取HGL345这样的一个句柄，获取成功则退出程序。该互斥量作用是保证同时只有一个该程序处于运行状态**

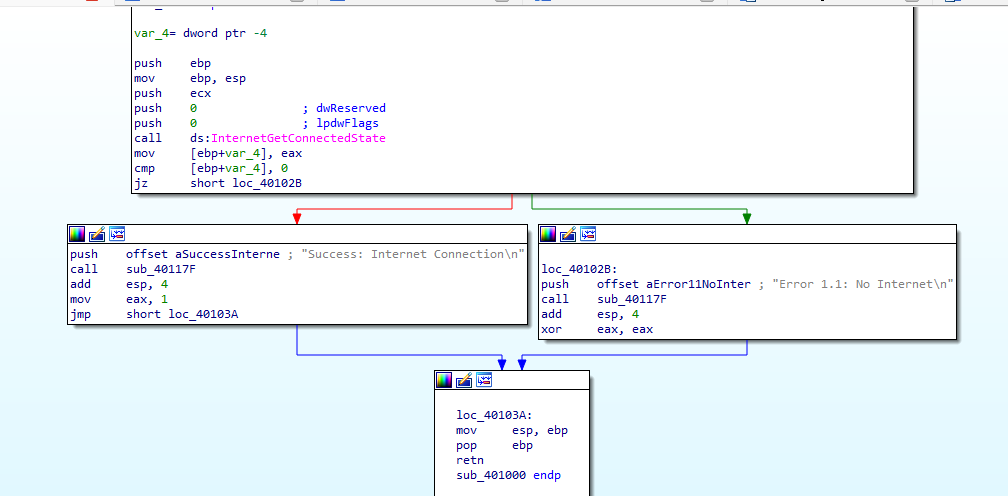
1. **HGL345句柄和Malserve服务**
2. **在下列代码中我们可以发现本程序开始设置一系列有关于时间的内容**



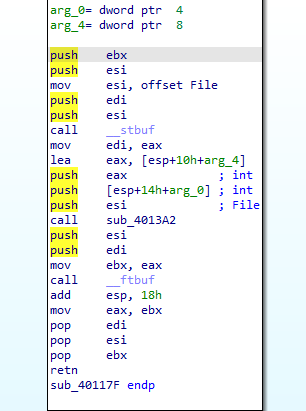
**在时间的部分设置为了2100年1月1日，之后调用SystemTimeToFileTime转换时间格式。之后程序开始等待，开始执行时发现了Internet Explorer 8.0和http://www.malwareanalysisbook.com可以作为网络特征**



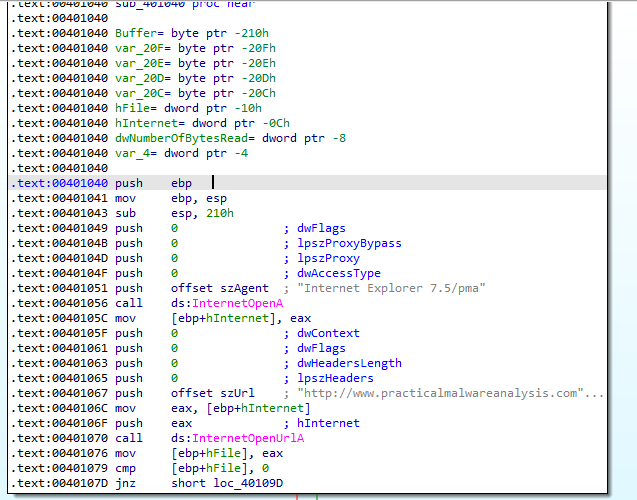
1. **如上文所述，本程序将等待到2100年1月1日并向http://www.malwareanalysisbook.com发送请求，看起来是DDOS攻击**
2. **2100年1月1日开始后不会停止**
3. **Lab06-02**
4. **是if函数，判断是否有网络链接**



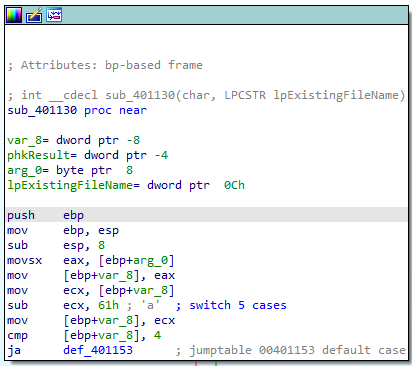
1. **调用了printf**



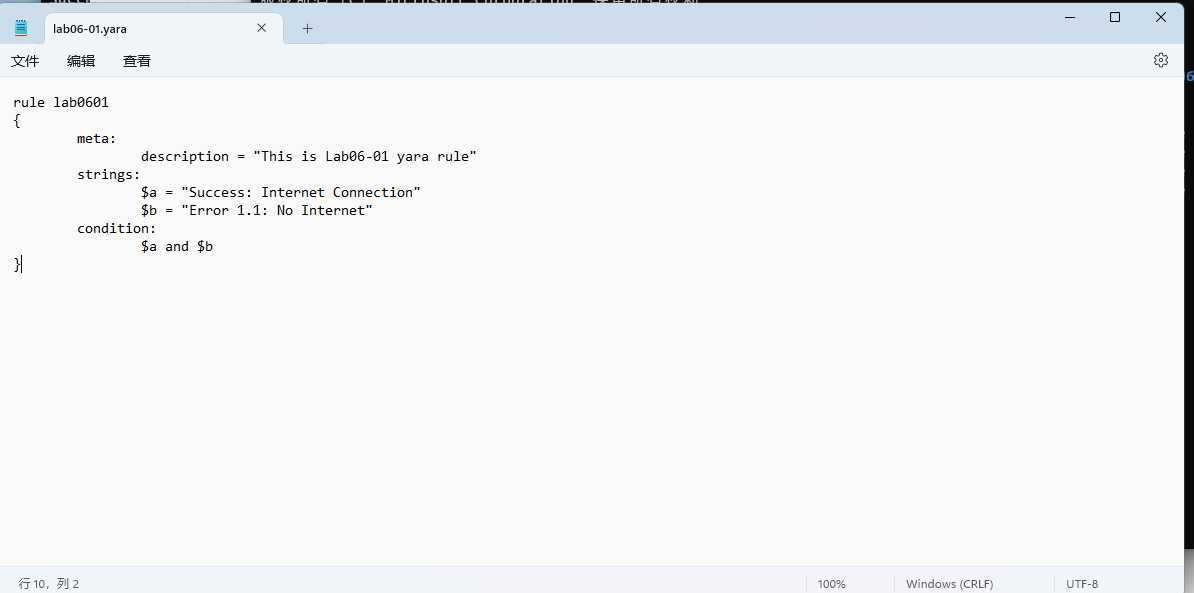
1. **从相关网址中下载内容**



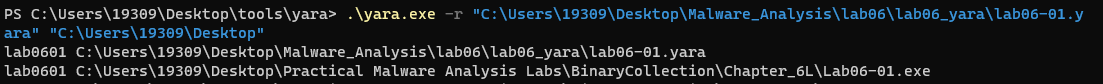
1. **调用InternetReadFile，将读到的字符存入字符数组**
2. **将Internet Explorer 7.5/pma作为User-Agent，从http://www.practicalmalwareanalysis.com下载网页**
3. **程序首先判断是否存在一个可用的Internet连接，如果不存在就终止运行。否则，程序使用一个独特的用户代理尝试下载一个网页。该网页包含了一段由<!--开始的 HTML注释，程序解析其后的那个字符并输出到屏幕,输出格式是“Success:Parsed command isX”,其中X就是从该HTML**
4. **Lab06-03**
5. **新增了0x401271函数为printf和0x401130**
6. **一个为从html的注释得来的指令字符，另一个为函数名本身**



1. **包含一个switch和一个跳转表**
2. **打印错误信息，删除文件，创建文件夹，设置注册表项值，复制文件或休眠**
3. **Software\\Microsoft\\Windows\\CurrentVe和C:\\Temp\\cc.exe可作为标志**
4. **该程序先检查是否存在有效的Internet连接。如果找不到，程序直接终止。否则，该程序会尝试下载一个网页,该网页包含了一段以<!--开头的HTML注释。该注释的第一个字符被用于switch语句来决定程序在本地系统运行的下一步行为，包括是否删除一个文件、创建一个目录、设置一个注册表run键、复制一个文件或者休眠100秒。**
5. **Lab06-04**
6. **检查了网络链接方法**
7. **增加了for循环**
8. **0x401040使用参数**
9. **运行24H**
10. **Internet Explorer 7.50/pma%d %d是指运行时间**
11. **首先，程序会检查是否有可用的Internet连接。如果找不到，程序就终止运行。否则，程序使用一个独特的User-Agent来下载一个网页，这个User-Agent包含了一个计数器，用于说明程序已经运行了多少分钟。下载下来的网页中包含了以<!--开头的HTML注释代码，这段注释代码中接下来的第一个字符被用于一个switch 语句，以决定接下来在本地系统的行为。其中包含了一些硬编码的行为，包括删除一个文件、创建一个目录、设置一个注册表run键、复制一个文件、休眠100秒等。该程序会运行24小时后终止。**
12. **Yara练习**
13. **Lab07-01**



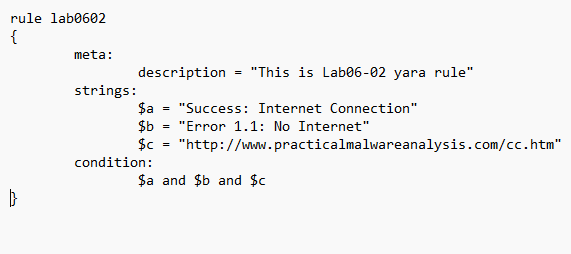
**运行后发现可成功抓取相应的恶意代码**



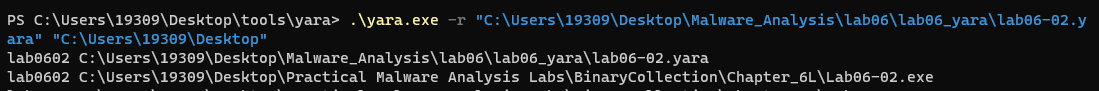
**共执行了7775.5306ms**



1. **Lab06-02**



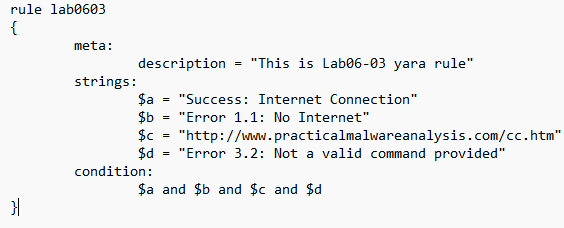
**运行后发现可成功抓取相应的恶意代码**



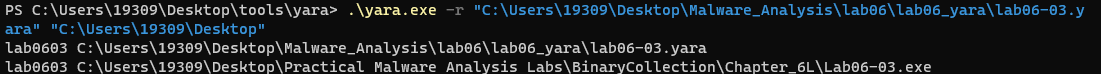
**共执行了2871.5047ms**



1. **Lab06-03**



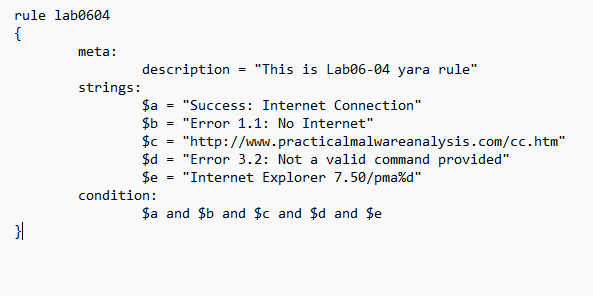
**运行后发现可成功抓取相应的恶意代码**



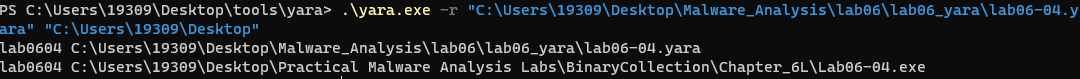
**共执行了6000.3624ms**



1. **Lab06-04**



**运行后发现可成功抓取相应的恶意代码**



**共执行了8614.8786ms**



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。**