

**恶意代码课程实验报告**

**实验五**

****

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

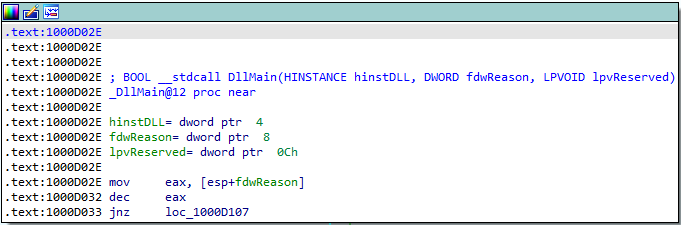
1. **实验环境**

VMWARE，Windows11

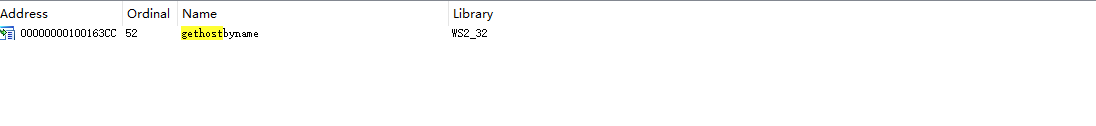
1. **实验工具**

STRINGS, PEVIEW，DEPENDENCY WALKER，EXEInfo，YARA

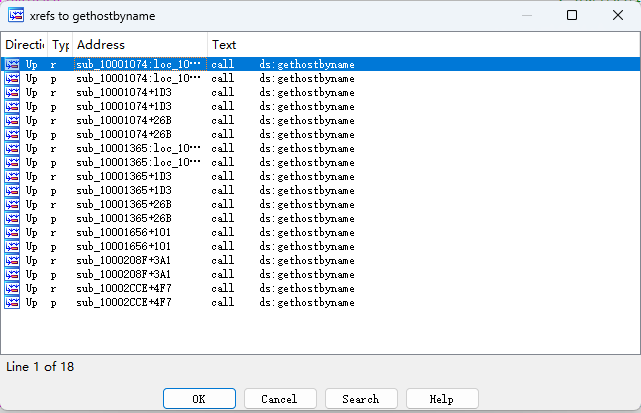
1. **实验过程**
2. **Lab5-1**
3. **IDA Pro打开文件，直接就可以进入到DllMain，可以发现该函数位于.text字段的0X1000D02E**

****

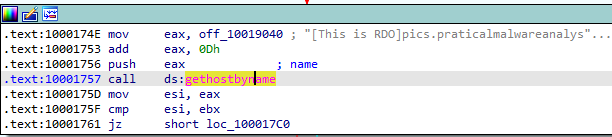
1. **发现gethostbyname地址位于0X100163CC**

****

1. **查看该函数的交叉引用如图，可以发现gethostbyname被5个不同的函数进行了调用，共调用了9次**

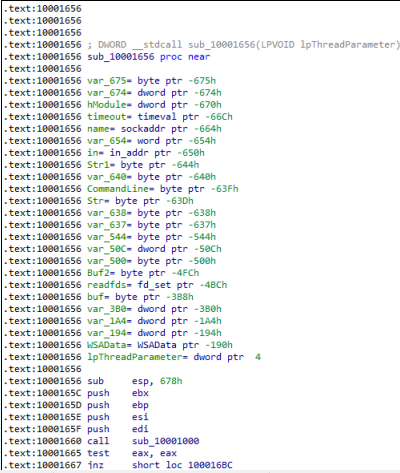


1. **跳转到相应地址可以发现如下代码**

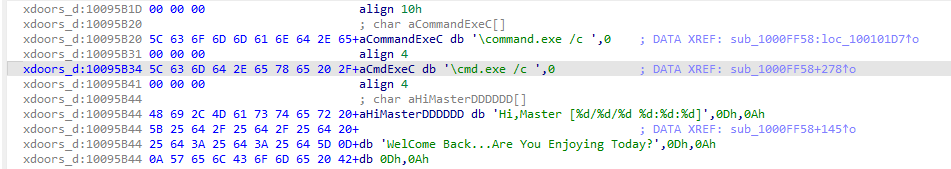
****

**在这里发现字符串[This is RDO]pics.praticalmalwareanalysis.com被赋值给了eax，而gethostbyname传入了eax中的地址，也就是说此时将会发起对praticalmalwareanalysis.com的DNS请求。代码中的第二行是为了跳过前面一部分无用的字符串**

1. **分析如下代码可以发现IDA识别出了23个局部变量**

****

1. **识别出了一个参数**
2. **使用String窗口进行查看发现位于0X10095B34**

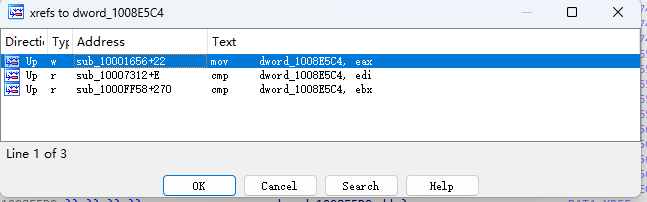
****

1. **可能是一个远程shell会话**
2. **首先来到0X100101C8处，可以发现如下代码**

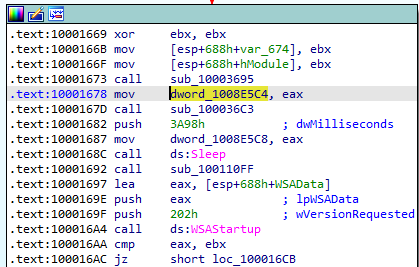
**屏幕截图 2023-10-15 174319**

**之后来到dword\_1008E5C4处，并未发现特殊，因此开始查看交叉引用**



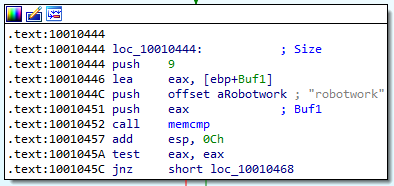


**发现在sub\_10001656+22处修改了dword\_1008E5C4，因此进入查看**



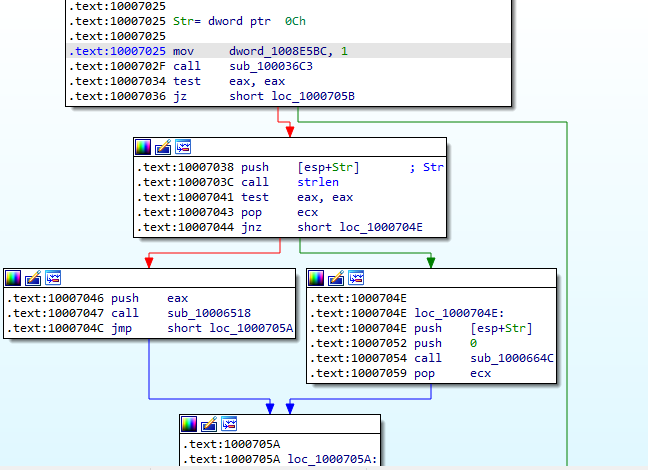
**查看在这一行之前的函数，发现是一个有关版本号的函数，也就是说，本程序对于此的修改应为存储版本号**

1. **我们可以找到如下代码**

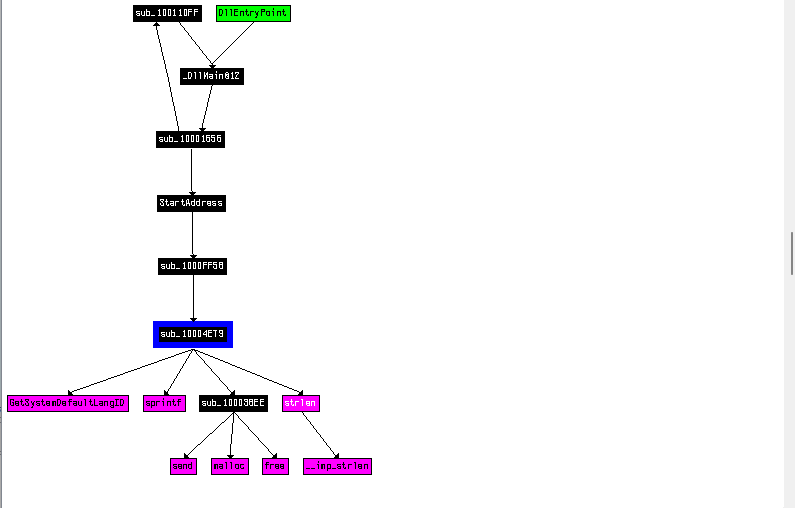


**也就是若字符串为robotwork就进行代码调用，经过查看最后将会查找在注册表的SOFTWARE\Microsoft\Windows\CurrentVersion\WorkTime会被查询并被发送**

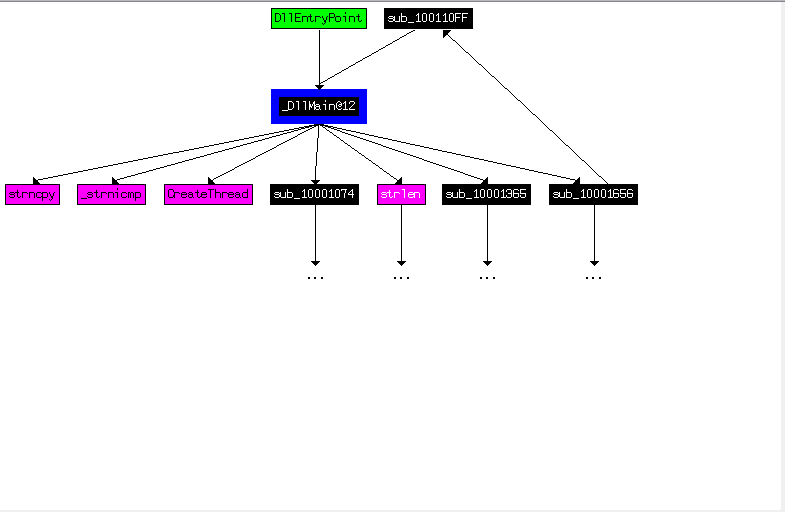
1. **该函数的流程图入下**

****

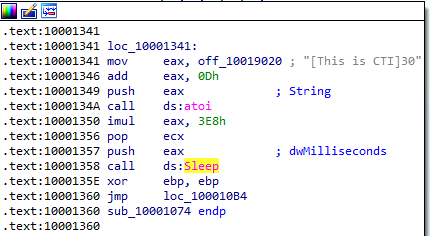
**也就是说他可以通过网络发送进程表或某一特定程序的状态**



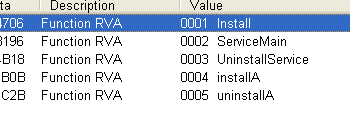


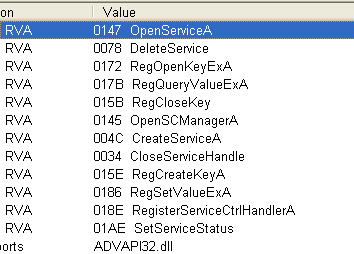


1. **有如下代码片段可知，首先eax先被赋值为30，之后乘上1000，也就是说最后将要休眠30秒**



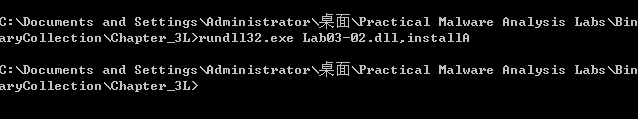
1. **6、1、2**
2. **IPPROTO\_TCP、SOCK\_STREAM、AF\_INET**
3. **0X100061DB、0X564D5868调用了in**
4. **看似是一些随机数**
5. **数据被反混淆得到字符串**
6. **发现字符串为xdoor is this backdoor, string decoded for Practical Malware Analysis Lab :)1234**
7. **对其0x50长度的字节数据，之后使用Practical函数进行修改**
8. **Lab3-2**
9. **使用PEview发现有5个导出函数和多个导入函数**





**通过对于这些函数的分析我们初步认为该程序会通过installA将自身安装成一个服务。**

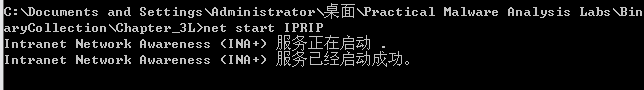
**使用rundll32.exe进行运行。**

****

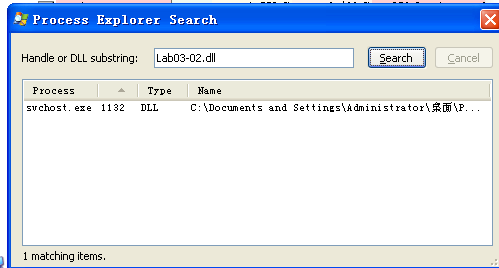
1. **使用regshot发现恶意程序已经将自己安装为IPRIP服务**



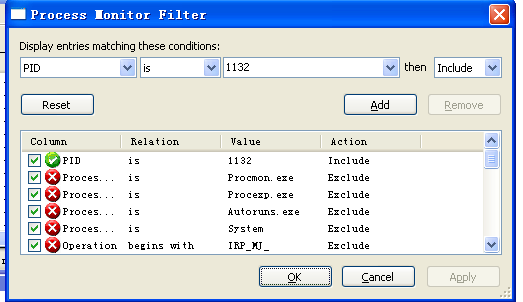
**之后使用net start IPRIP就可以运行**



1. **使用process expoler发现服务运行在svchost.exe下**



1. **设置成PID过滤**



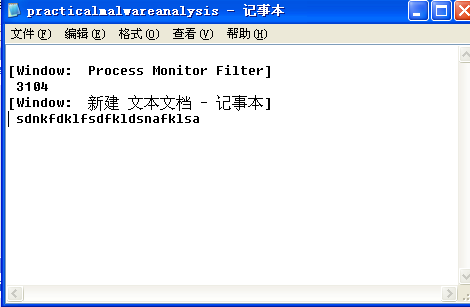
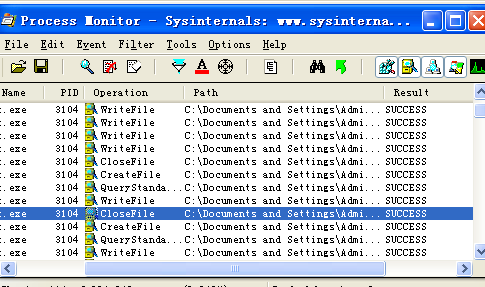
1. **恶意代码会将自身安装成IPRIP服务，会将自身永久安装在注册表上。**
2. **会解析相应域名，同时占用80接口，并使用GET请求。**
3. **Lab3-3**
4. **使用process explorer发现使用后出现单独的svchost.exe，也就是说实现了对此文件的替换**

**屏幕截图 2023-10-05 234314**

1. **对svhost.exe进行了替换**
2. **创建名为practicalmalwareanalysis的文件**

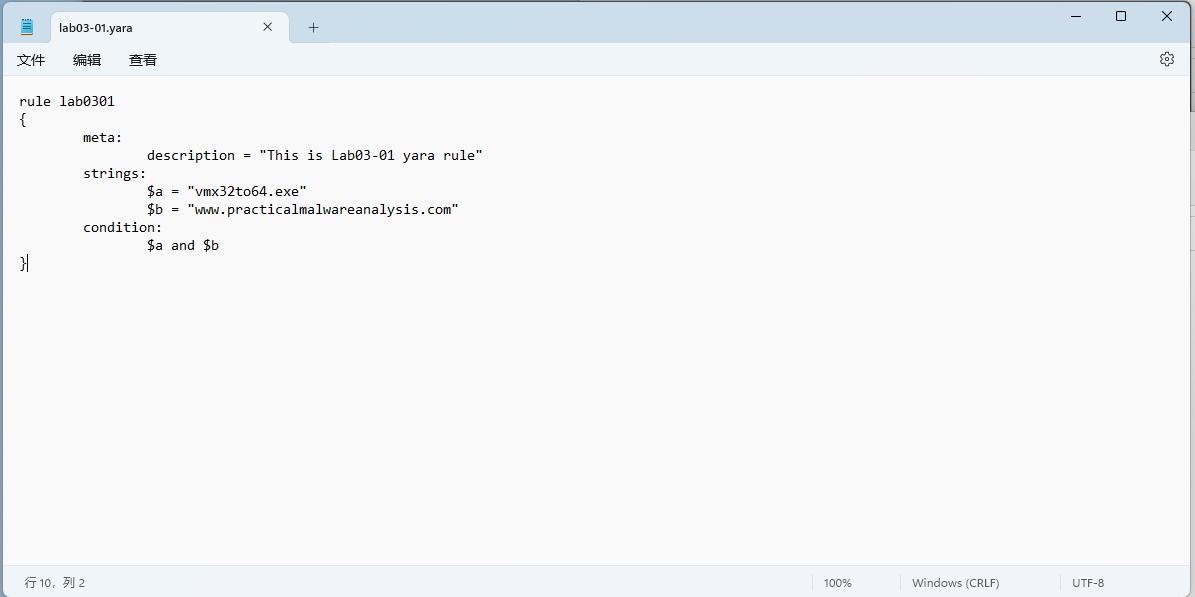


1. **打开创建的文件，同时在process monitor执行过滤相应程序的pid，发现该程序会统计击键的情况**

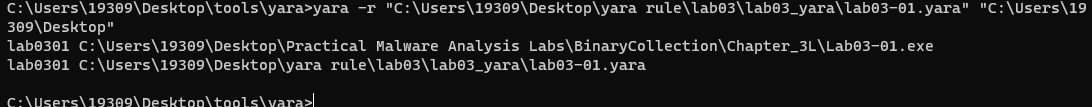
****

1. **Lab3-4**
2. **运行后将自身删除**
3. **无法分析，怀疑缺少某些命令**
4. **没有**
5. **Yara练习**
6. **Lab03-01**

**经调查发现，在本程序中存在vmx32to64.exe和www.practicalmalwareanalysis.com两个特殊字符串，因此构造如下的yara规则：**



**运行后发现可成功抓取相应的恶意代码**

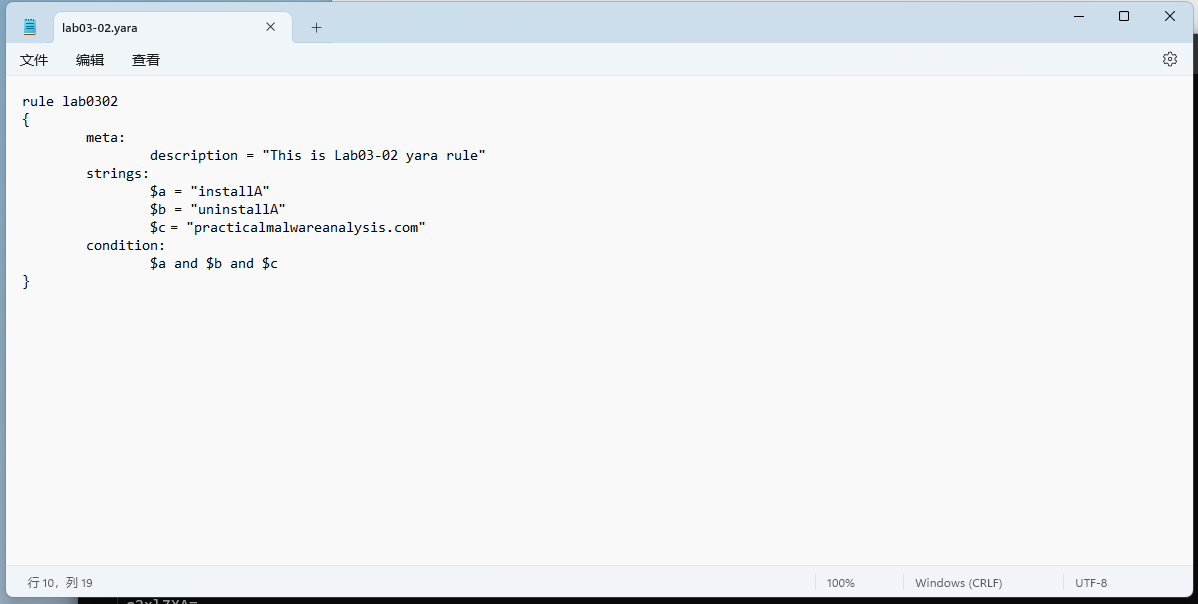


**共执行了2094.0252ms**

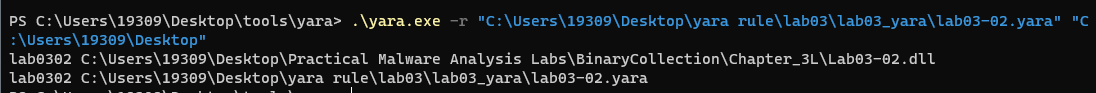


1. **Lab03-02**

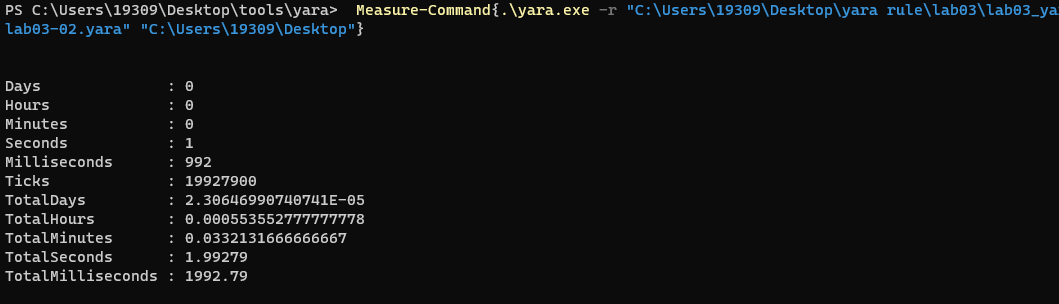
**我们发现该程序中有以下有趣的字符串：installA，uninstallA，practicalmalwareanalysis.com，并据此生成相应规则：**



**运行后发现可成功抓取相应的恶意代码**

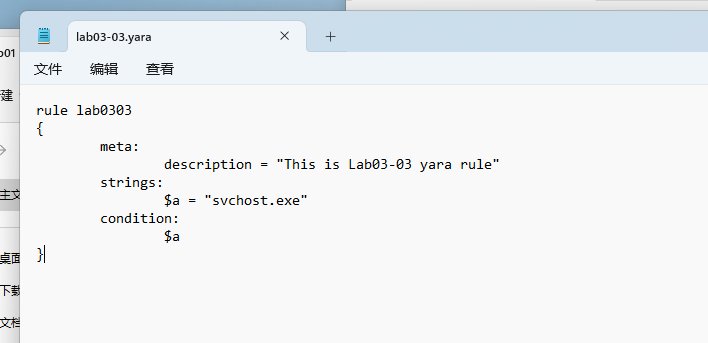


**共执行了1992.79ms**

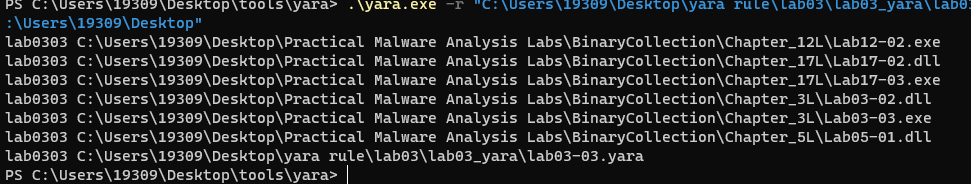


1. **Lab03-03**

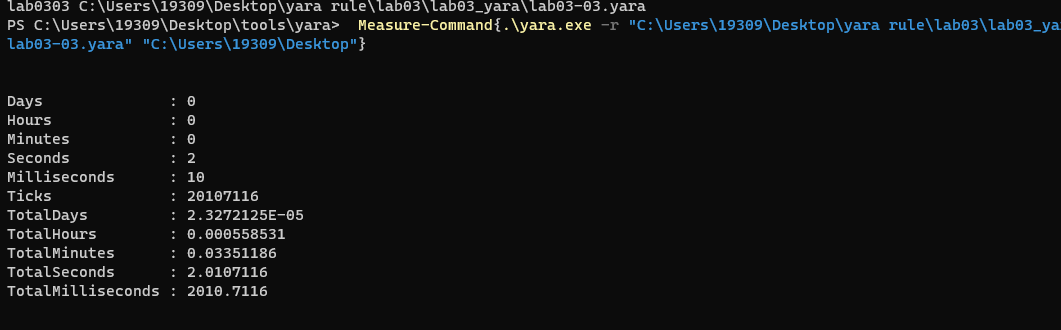
**发现该文件中字符串均为乱码，通过表现特性猜测其中可能有svchost.exe这种特殊字符串，因此构造如下规则：**



**运行后发现可成功抓取相应的恶意代码，但同时抓取了其它恶意代码。**

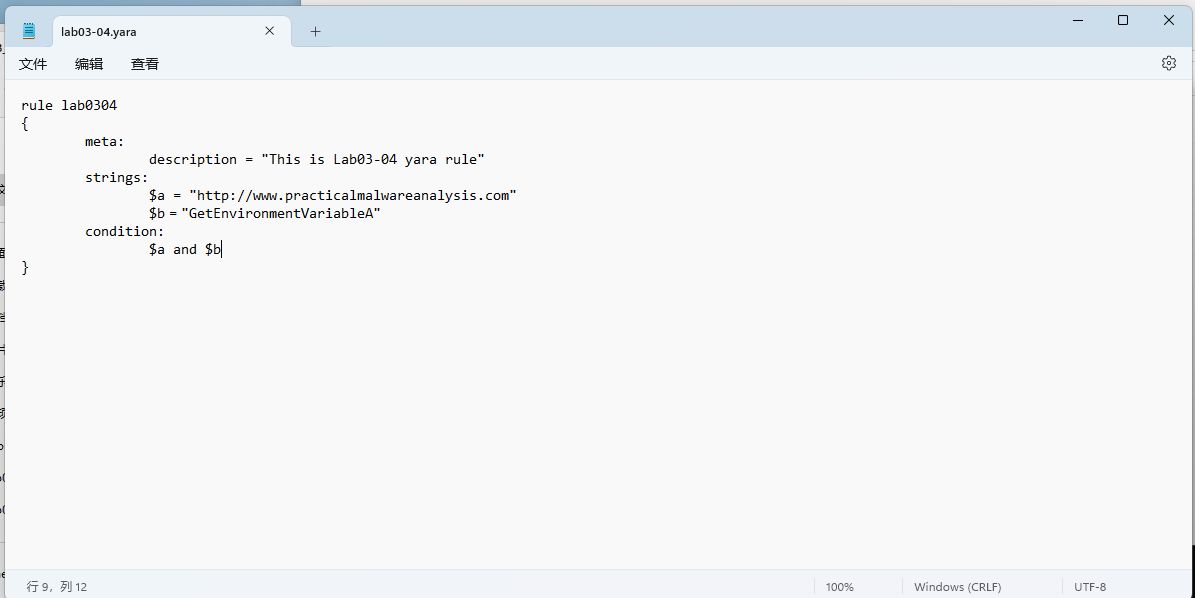


**共执行了2010.7116ms**

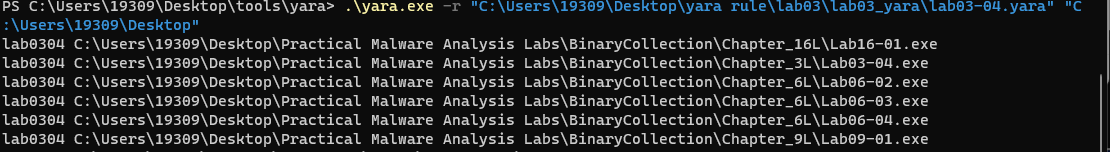


1. **Lab03-04**

**发现了http://www.practicalmalwareanalysis.com和GetEnvironmentVariableA两个特殊字符串。据此构建的yara规则如下：**



**运行后发现可成功抓取相应的恶意代码**



**共执行了2110.0373ms**



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。**