

**恶意代码课程实验报告**

**实验三**

****

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

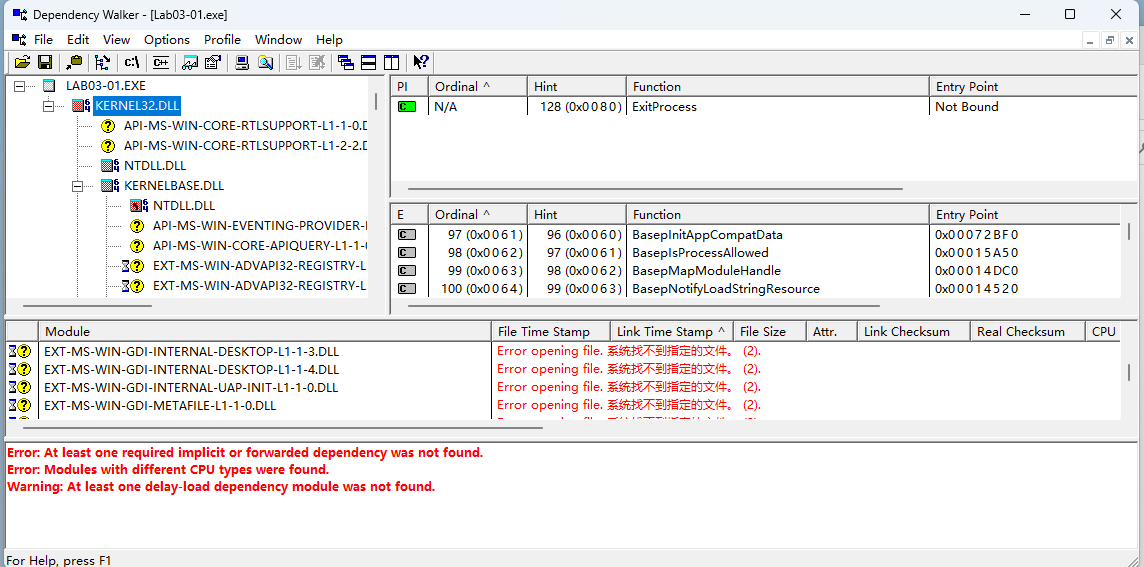
1. **实验环境**

VMWARE，Windows11

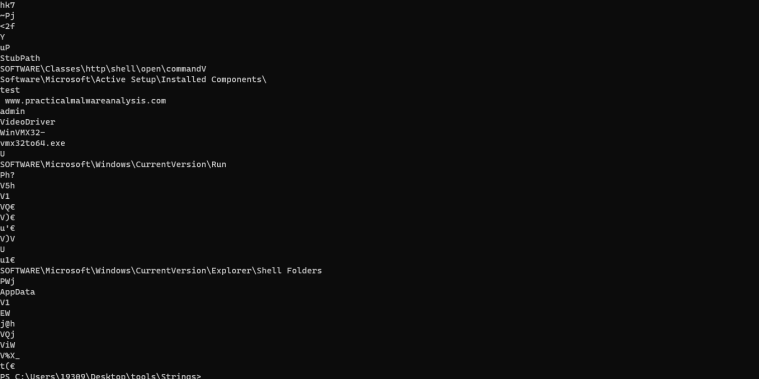
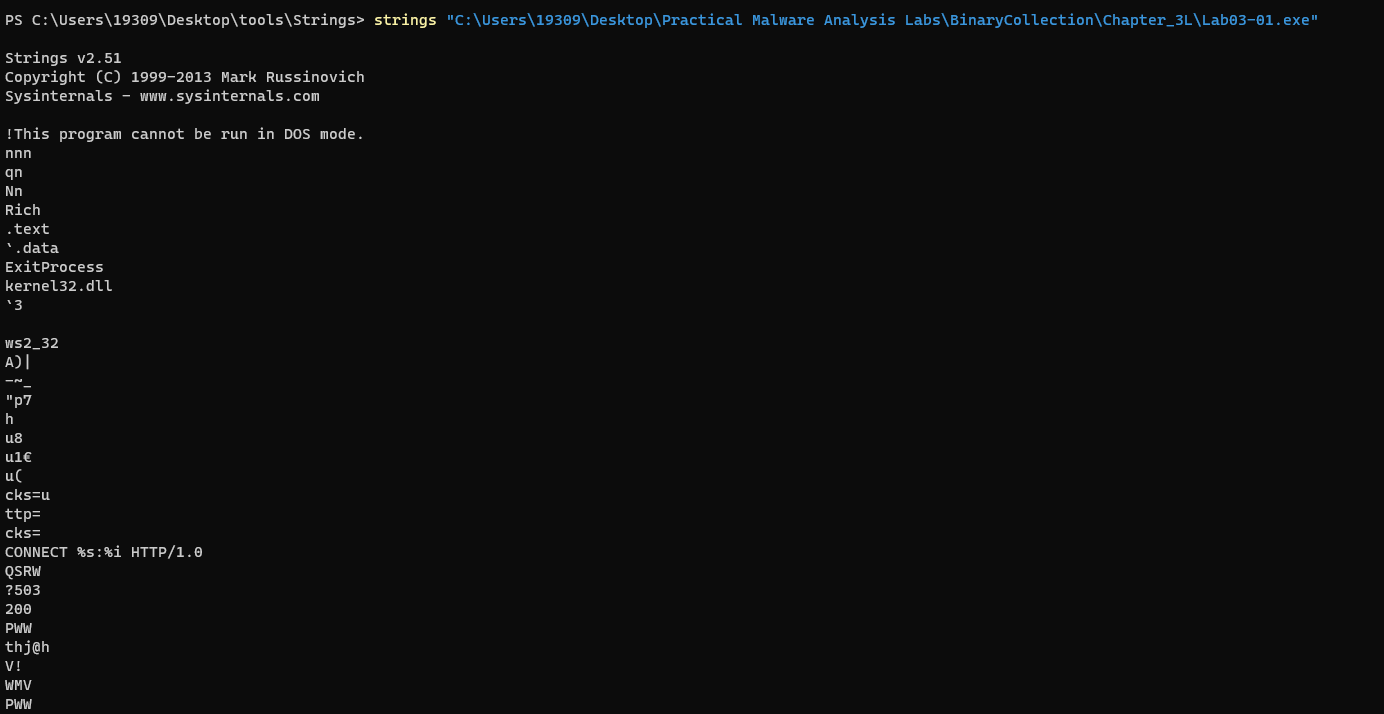
1. **实验工具**

STRINGS, PEVIEW，DEPENDENCY WALKER，EXEInfo，YARA

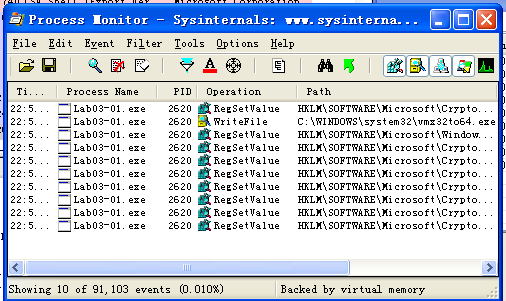
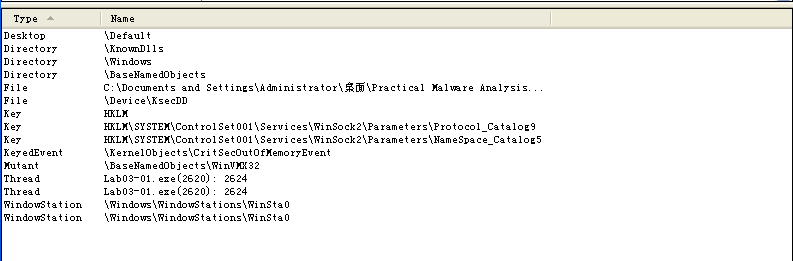
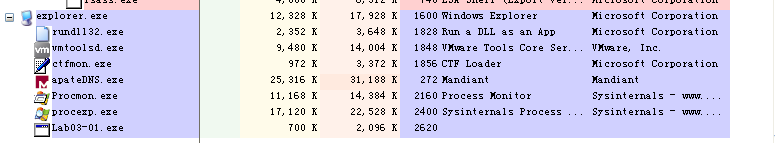
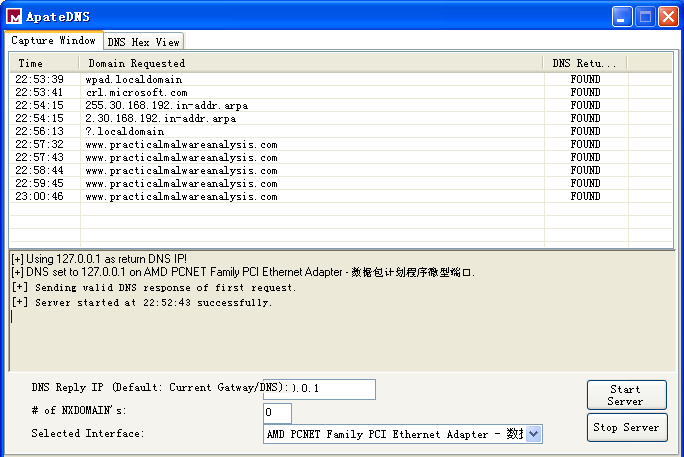
1. **实验过程**
2. **Lab3-1**
3. **使用Dependency Walker打开相关程序，发现其中的导入函数如下图，有且只有ExitProcess一个函数**



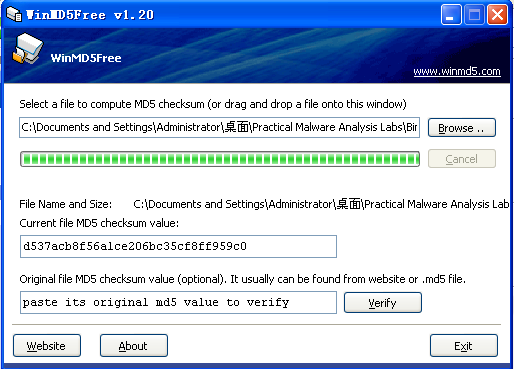
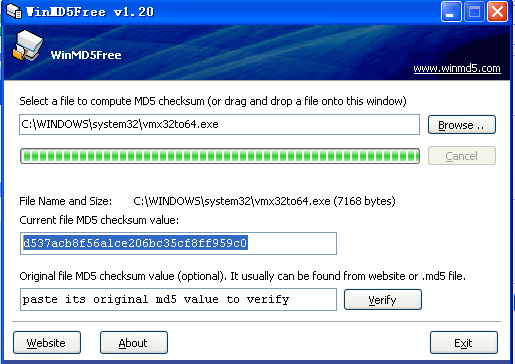
**使用Strings工具发现其中的字符串如下图，仅能发现此程序需要联网，同时似乎表明该程序被加壳。**

****

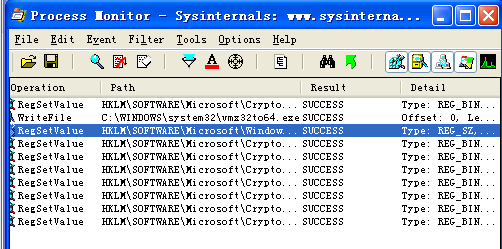
1. **使用Process Monitor和Process Explorer进行监视，并启用ApdateDNS。在运行程序后发现该程序一直向www.practicalmalwareanalysis.com发送请求，同时也能通过过滤发现该程序想系统启动程序中添加了一个名为vmx32to64的文件。**

****

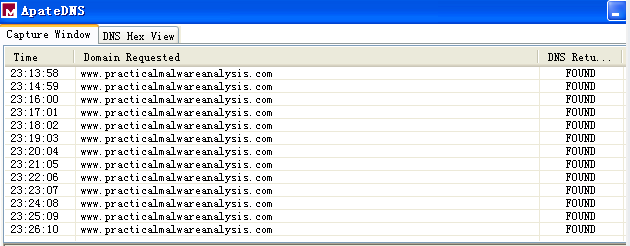
**使用winMD5Free分析新添加程序和原始程序的MD5值发现，二者均为d537acb8f56a1ce206bc35cf8ff959c0，可以说明原始程序通过复制自身将自己加入到了操作系统启动程序中。**

****

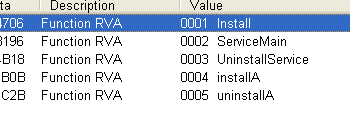
**同时发现该程序修改了注册表值为HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDrive，并将此处作为将要复制到的地址。**

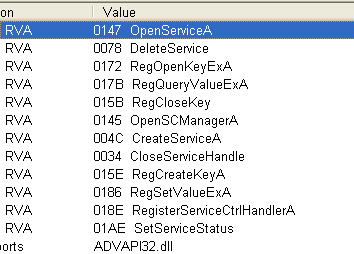


1. **使用AdateDNS发现该程序运行后一直向www.practicalmalwareanalysis.com进行解析并发送请求。**



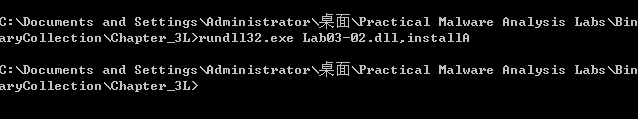
1. **Lab3-2**
2. **使用PEview发现有5个导出函数和多个导入函数**





**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。**

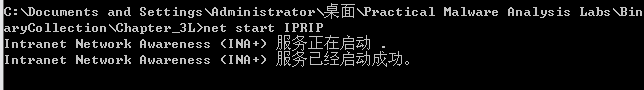
**使用rundll32.exe进行运行。**

****

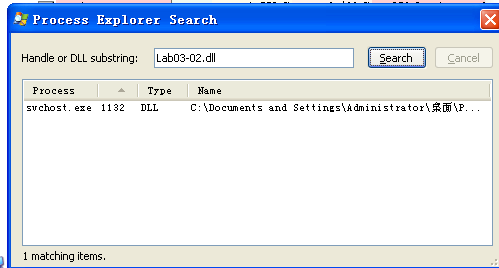
1. **使用regshot发现恶意程序已经将自己安装为IPRIP服务**



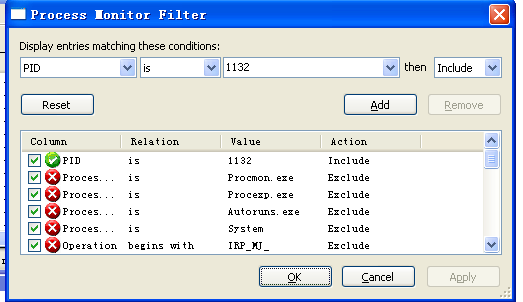
**之后使用net start IPRIP就可以运行**



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



1. **设置成PID过滤**



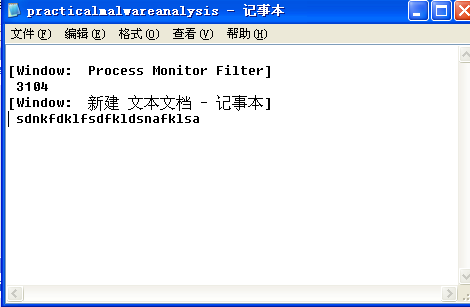
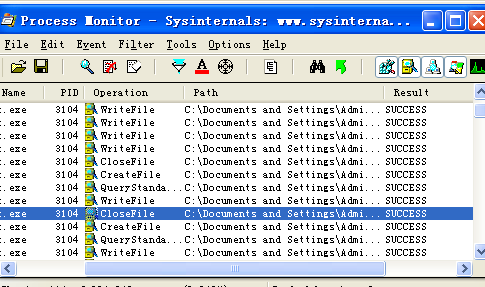
1. **恶意代码会将自身安装成IPRIP服务，会将自身永久安装在注册表上。**
2. **会解析相应域名，同时占用80接口，并使用GET请求。**
3. **Lab3-3**
4. **使用process explorer发现使用后出现单独的svchost.exe，也就是说实现了对此文件的替换**

**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**

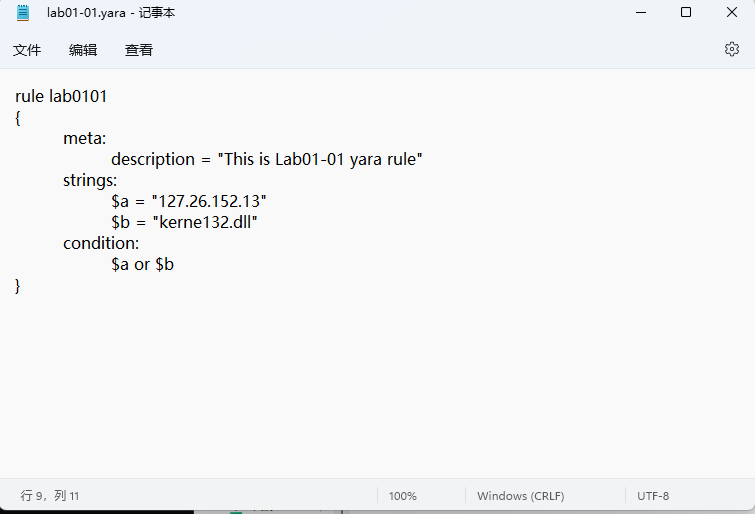


1. **打开创建的文件，同时在process monitor执行过滤相应程序的pid，发现该程序会统计击键的情况**

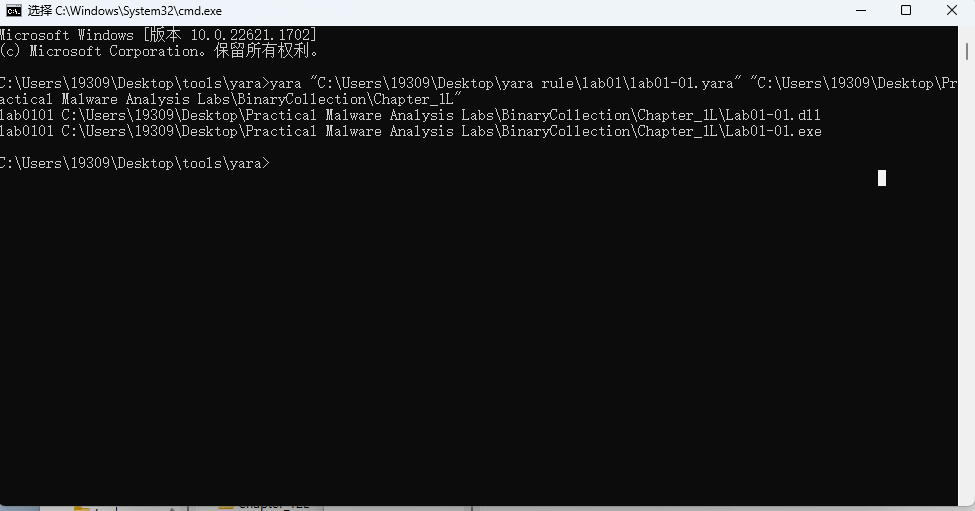
****

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. **Lab01-01**

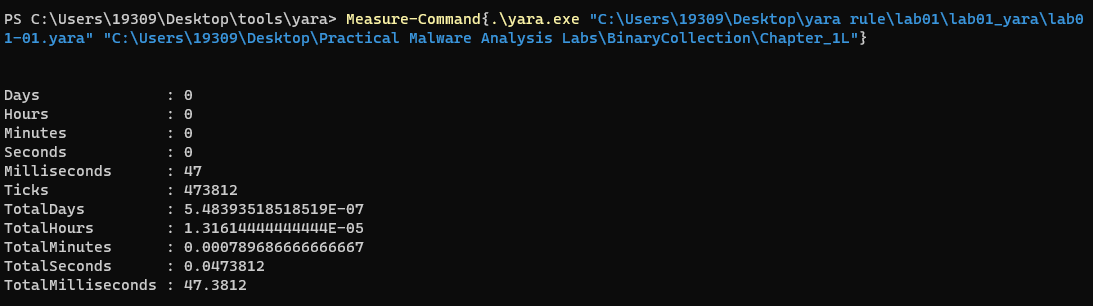
**经调查发现，在.dll文件中存在特殊字符串ipv4地址：127.26.152.13，；而在.exe文件中存在程序意欲创建的特殊文件名称：kerne132.dll。据此可以编写yara规则如下：**



**运行后发现可成功抓取相应的恶意代码**

****

**共执行了47.3812ms**

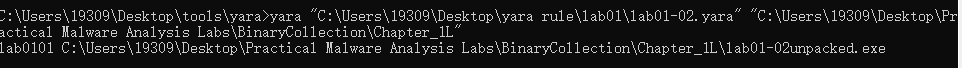


1. **Lab01-02**

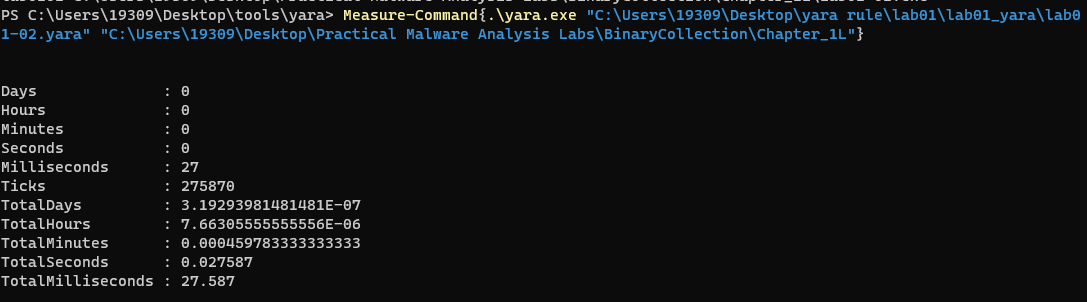
**经脱壳后发现该文件中存在http://www.malwareanalysisbook.com这一特殊网址以及Internet Explorer 8.0这一特殊字符串，据此可以编写yara规则如下：**



**运行后发现可成功抓取相应的恶意代码**

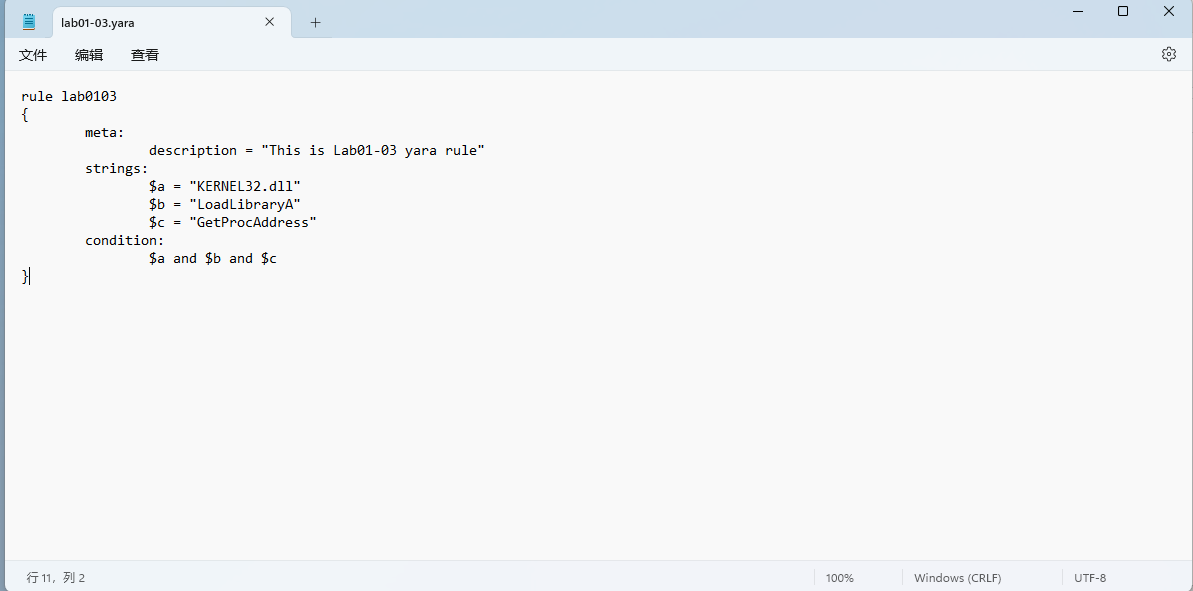


**共执行了27.587ms**

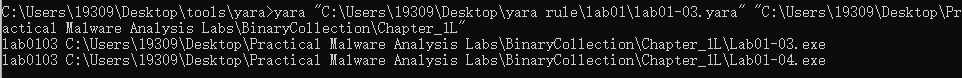


1. **Lab01-03**

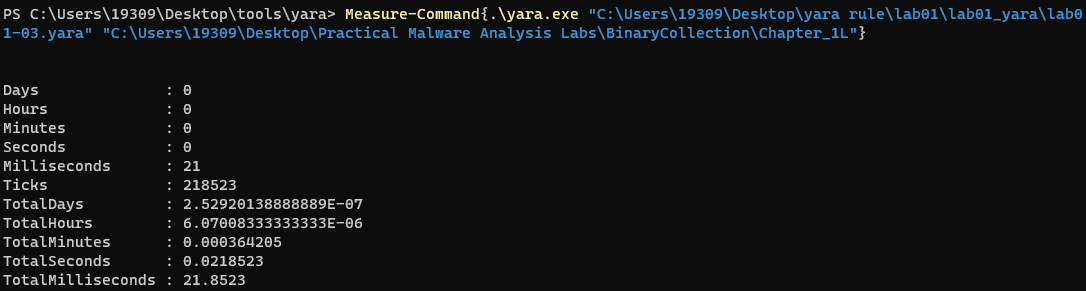
**发现以下特殊字符串：KERNEL32.dll、LoadLibraryA、GetProcAddress。最终构建的yara规则如下：**



**运行后发现可成功抓取相应的恶意代码，但同时抓取了其它恶意代码。**

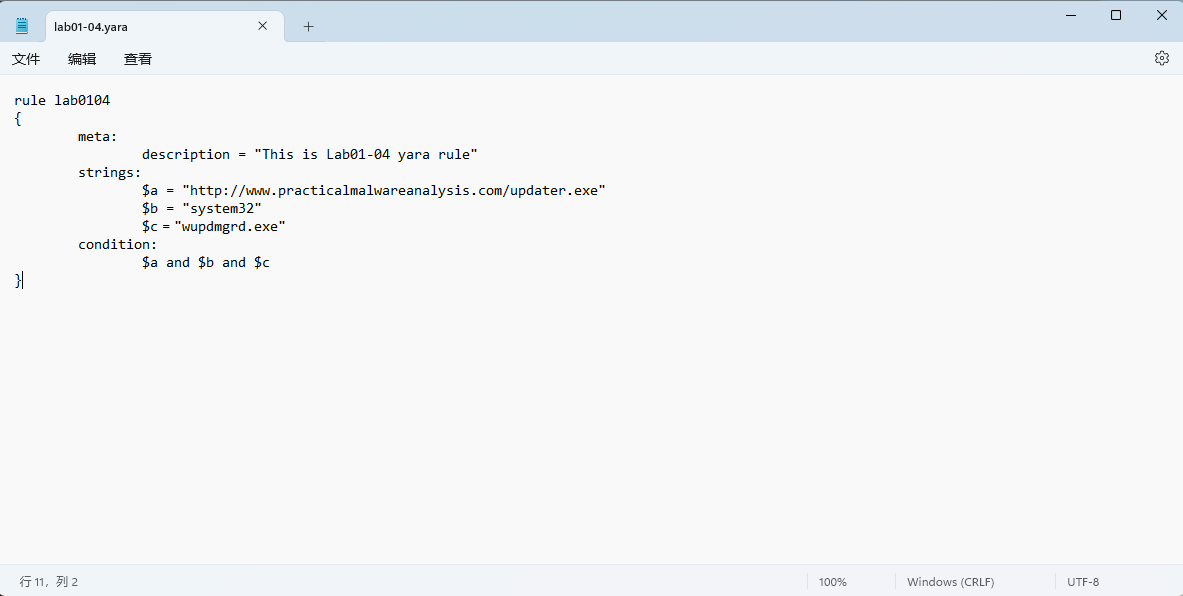


**共执行了21.8523ms**

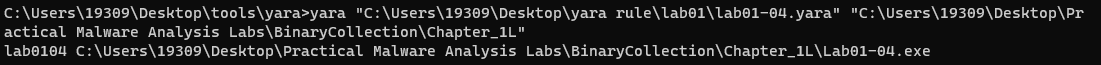


1. **Lab01-04**

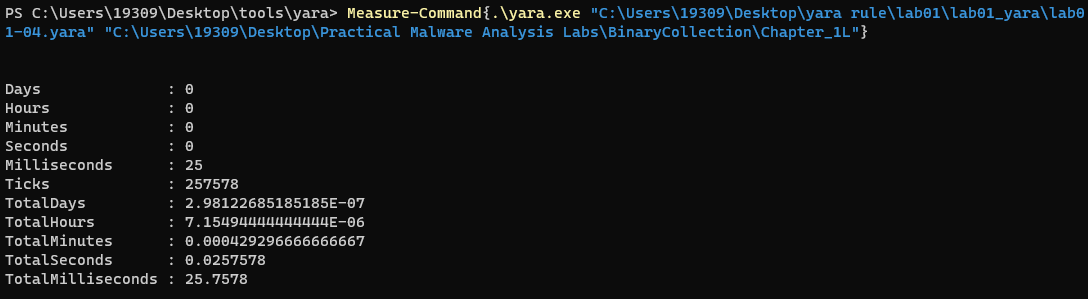
**发现了\system32\wupdmgrd.exe和http://www.practicalmalwareanalysis.com/updater.exe两个特殊字符串。据此构建的yara规则如下：**



**运行后发现可成功抓取相应的恶意代码**



**共执行了25.7578ms**



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。**