

**恶意代码课程实验报告**

**实验一**

****

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

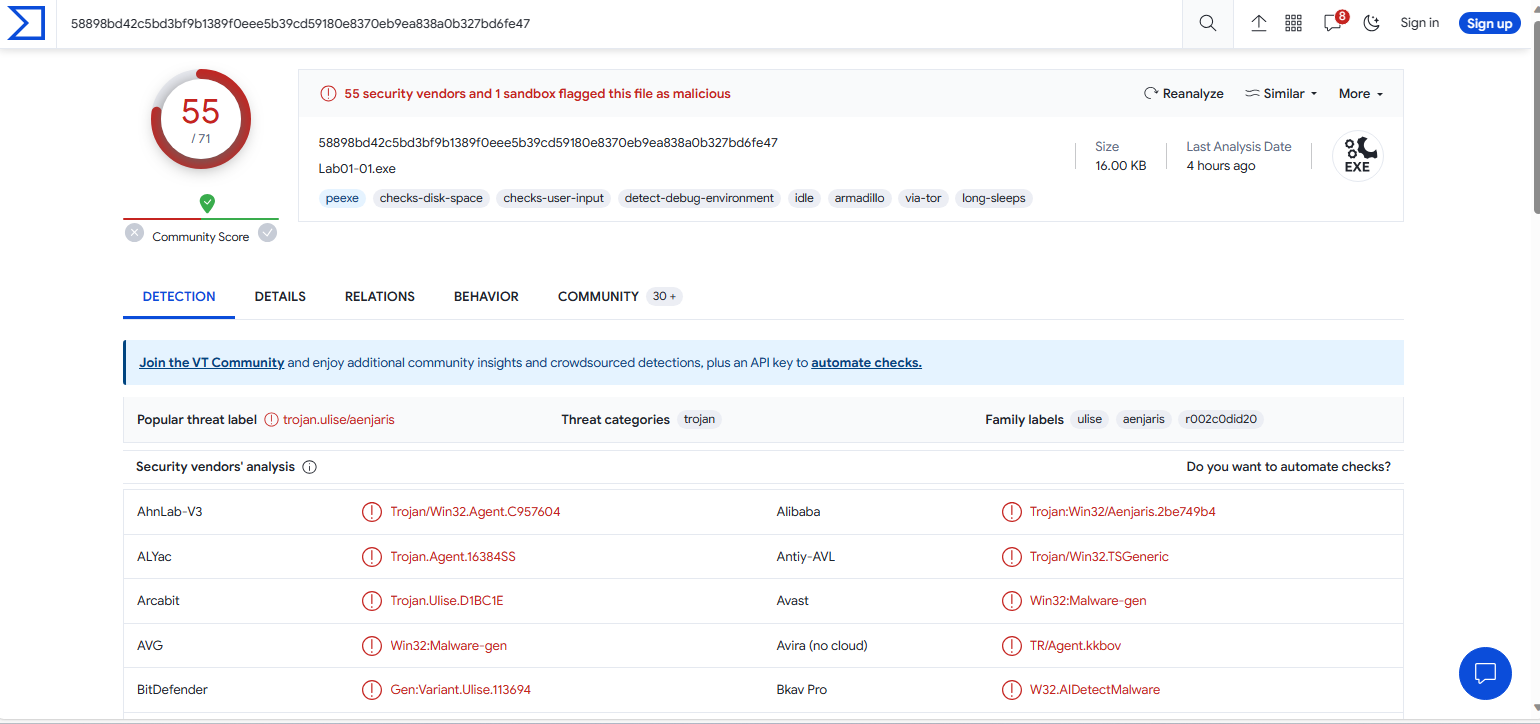
1. **实验环境**

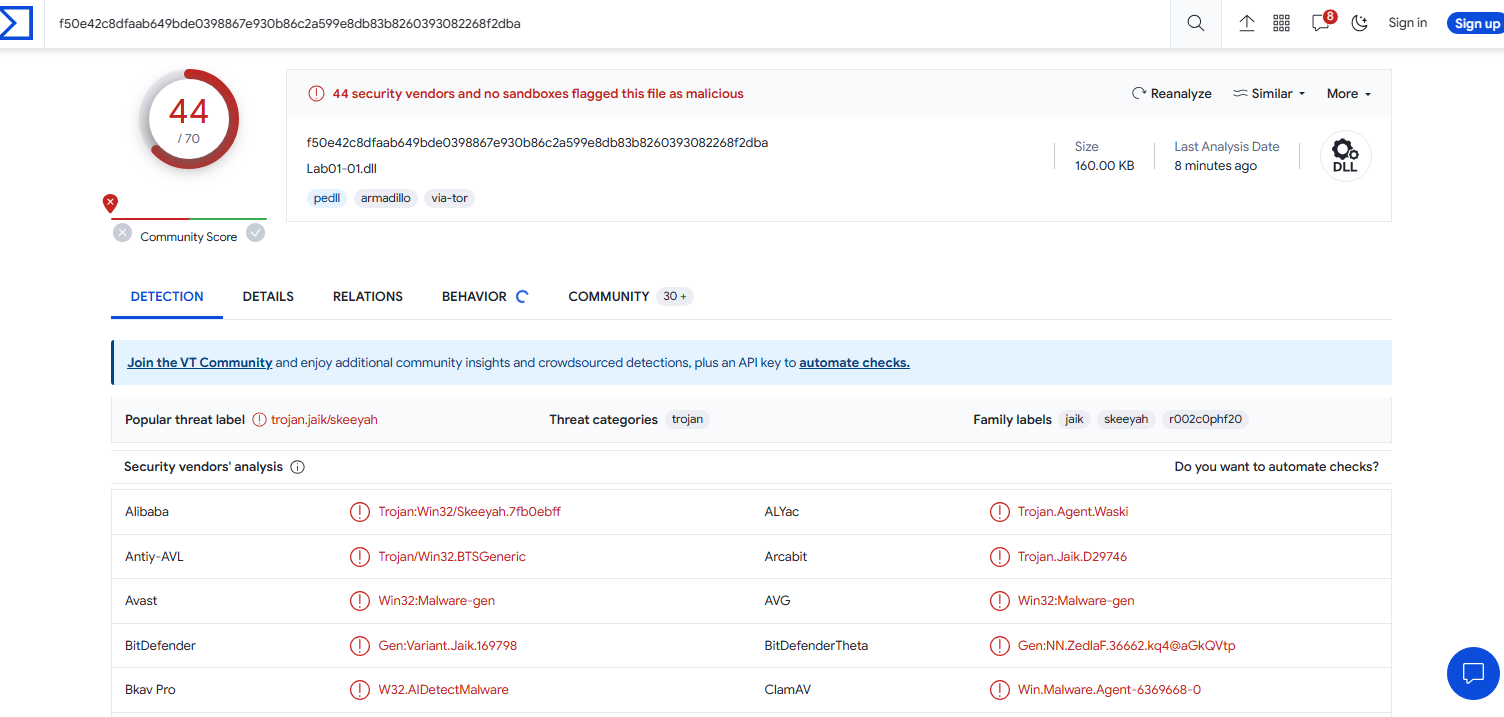
VMWARE，Windows11

1. **实验工具**

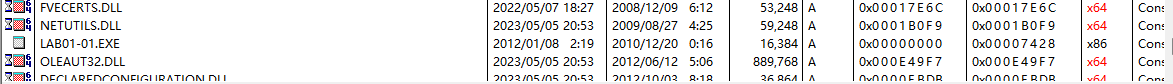
STRINGS, IDAPro,PEVIEW，EXEInfo，YARA

1. **实验过程**
2. **Lab1-1**
3. **上传后发现识别出了恶意代码**

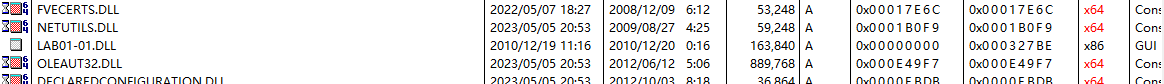
****

****

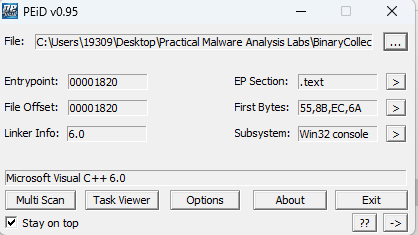
1. **Lab01-01.exe编译时间为2012/01/08 2：19**

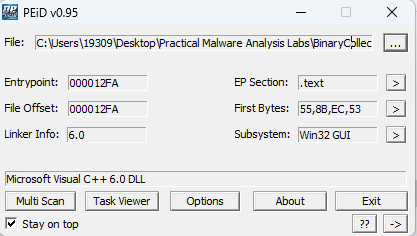
****

**Lab01-01.dll编译时间为2010/12/19 11：16**

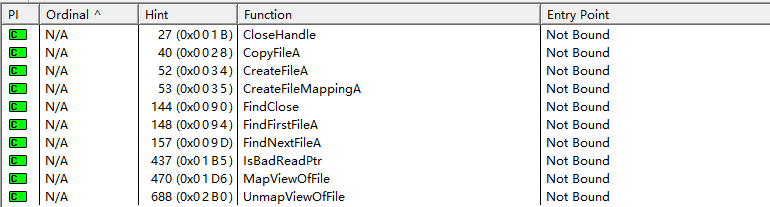


1. **两程序均未被加壳或混淆**

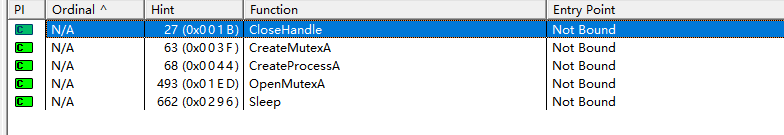




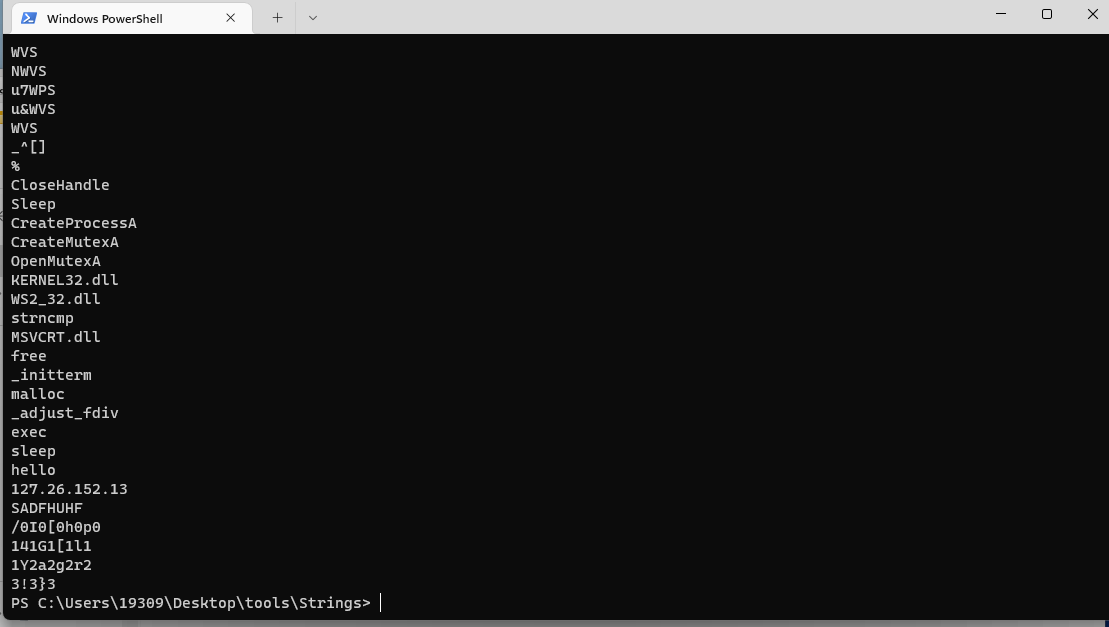
1. **Lab01-01.exe的导入函数中CopyFileA、FindFirstFileA、FindNextFileA可以显示该程序大概率是在系统中不断循环复制该文件。**

****

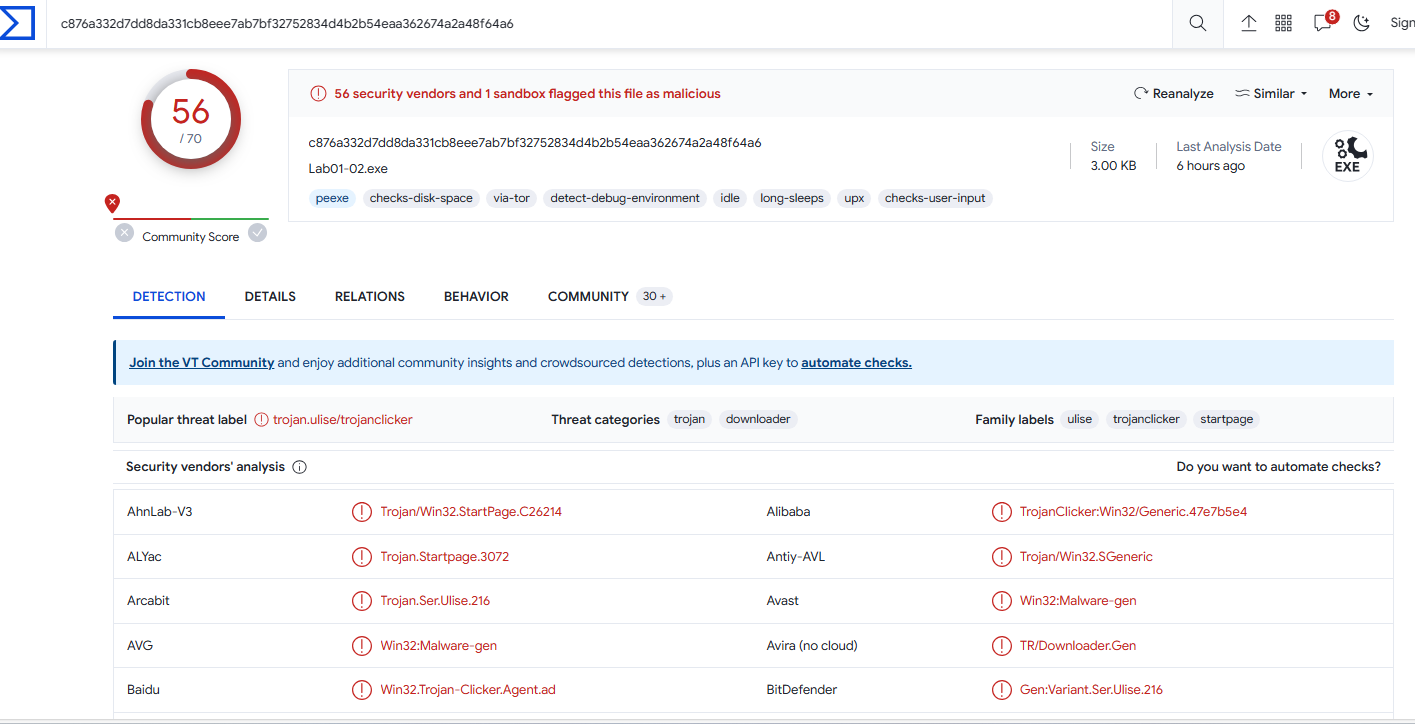
**Lab01-01.dll的导入函数中CreateMutexA、CreateProcessA、OpenMutexA、Sleep可以显示该程序大概率是将系统中的某些文件进行锁定。**



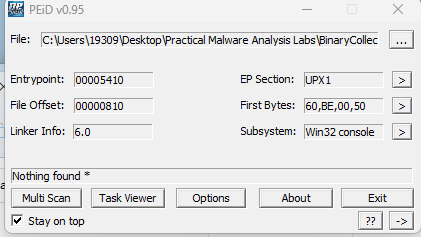
1. **可以通过检查kerne123.dll进行发现**
2. **在Lab01-01.dll中可以发现一个ipv4地址：127.26.152.13，可以据此进行恶意代码的发现。**

****

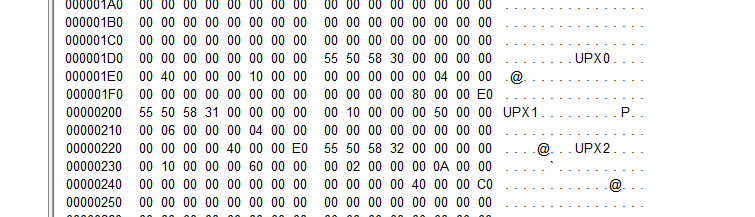
1. **我认为Lab01-01.dll是一个网络后门，Lab01-01.exe用于下载相关文件。**
2. **Lab1-2**
3. **上传后识别出了恶意代码**

****

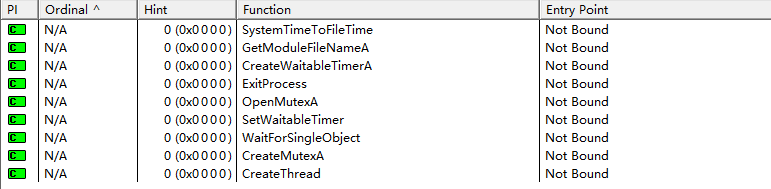
1. **被加壳**

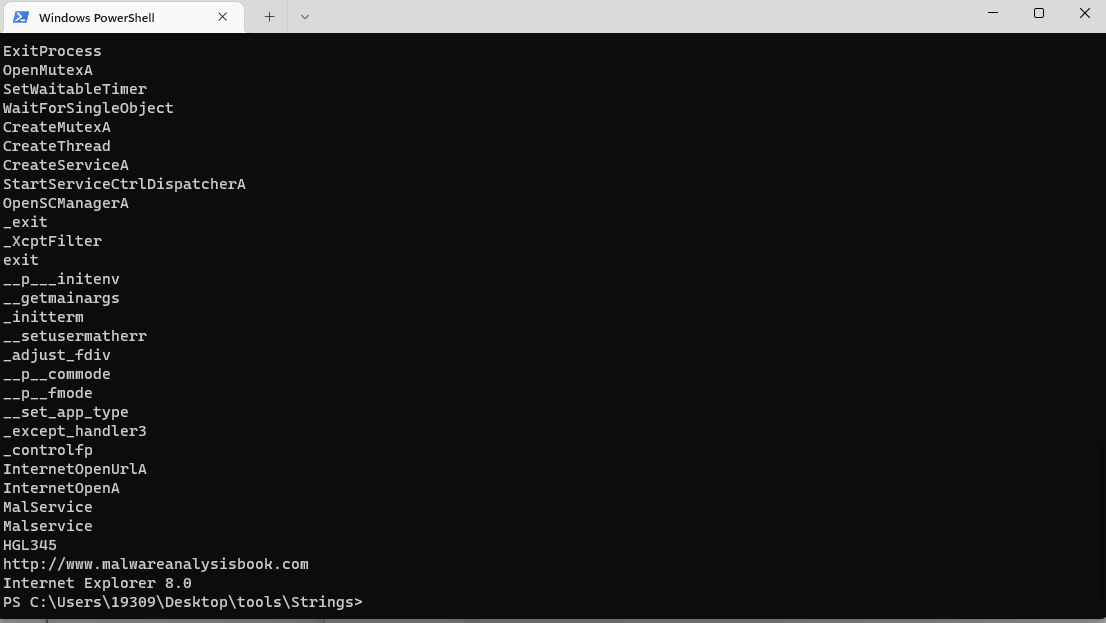


通过PEvie发现可能是UPX加壳

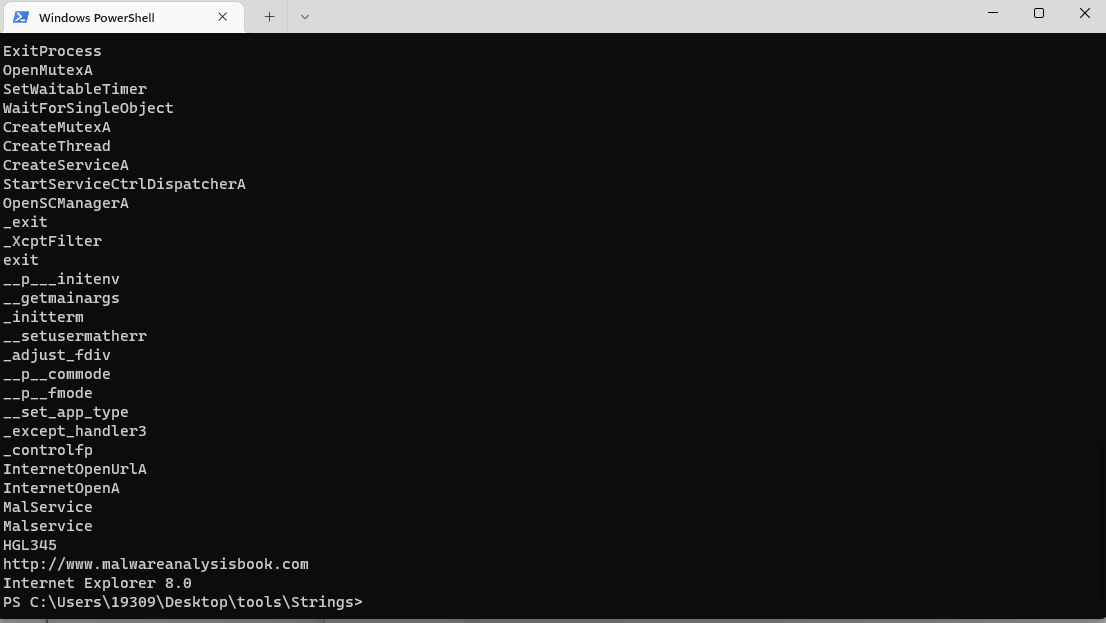


1. **脱壳后发现了如下函数，功能可能是打开网页创建服务**

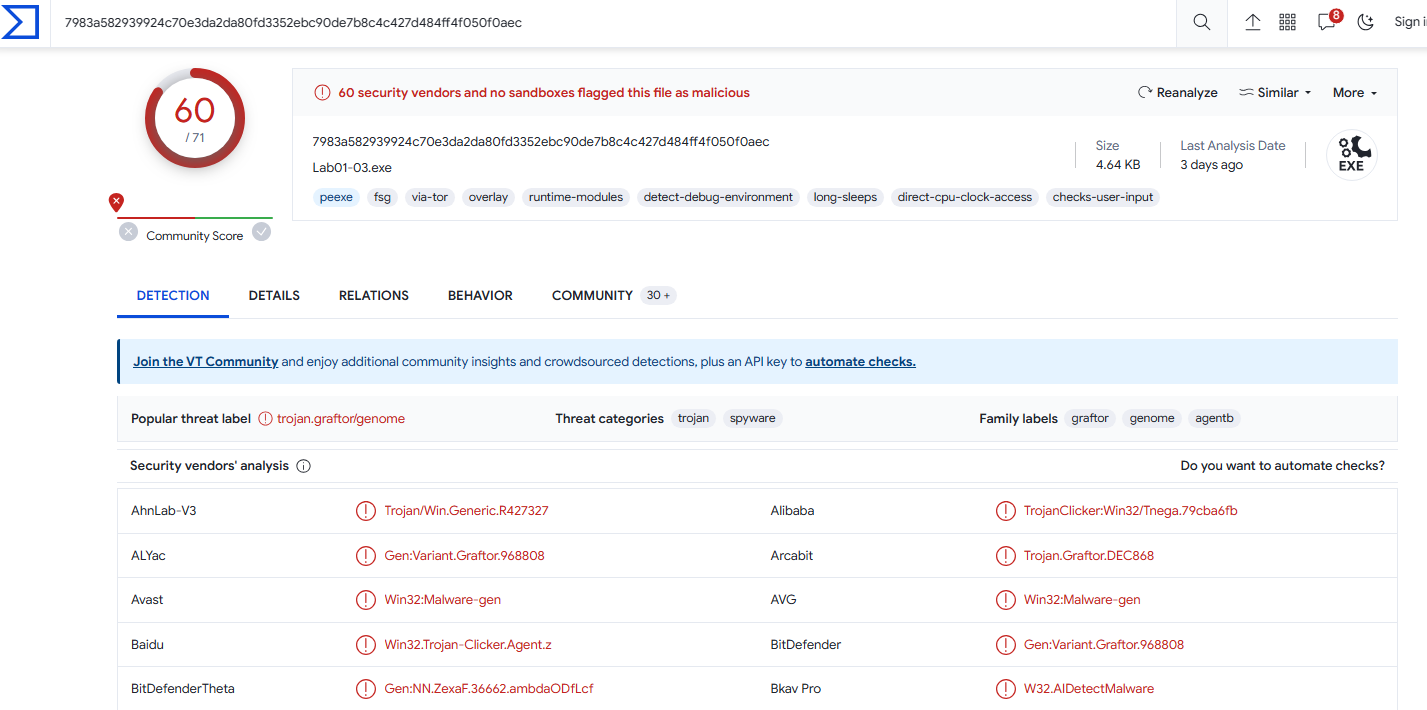




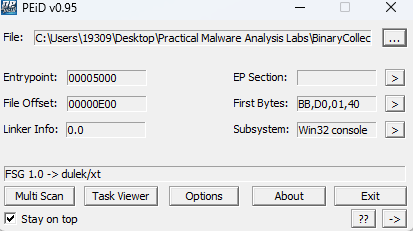
1. **通过Malservice 和到<http://www.malwareanalysisbook.com的流量进行判断>**



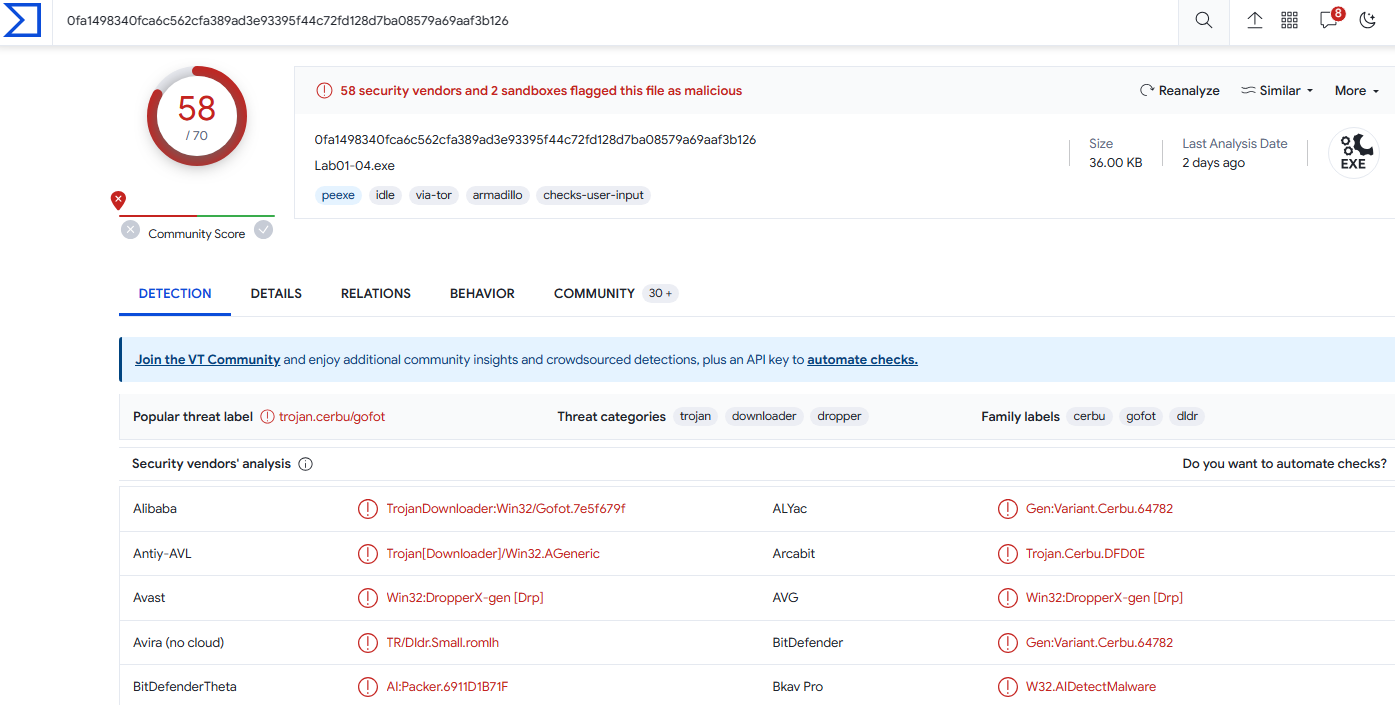
1. **Lab1-3**
2. **上传后识别出了恶意代码**



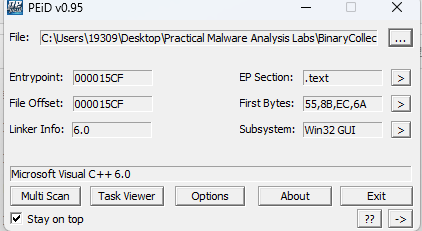
1. **是加壳的**



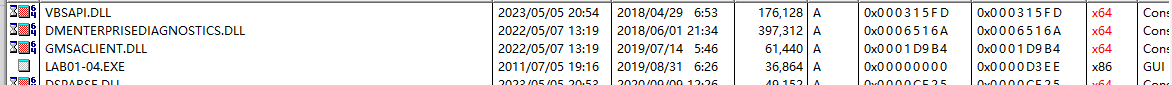
1. **无法脱壳，无法执行**
2. **无法脱壳，无法执行**
3. **Lab1-4**
4. **上传后识别出了恶意代码**



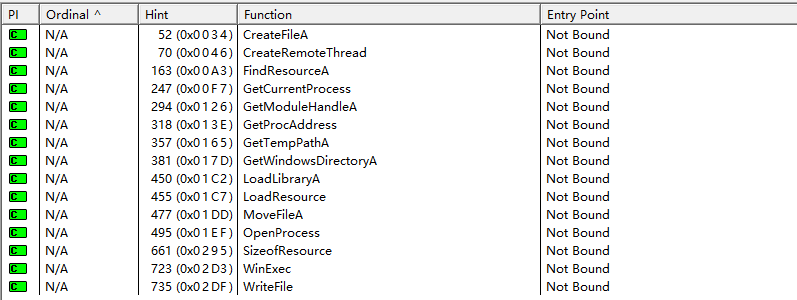
1. **未加壳**



1. **编译时间为2011/7/5 19：16**



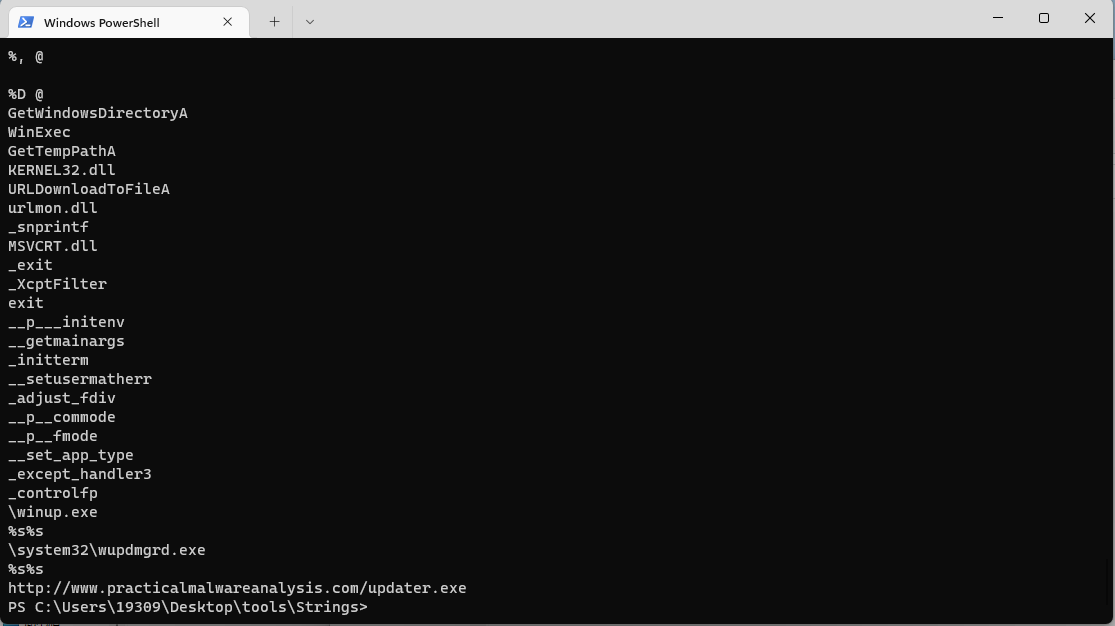
1. **发现以下导入函数**

****

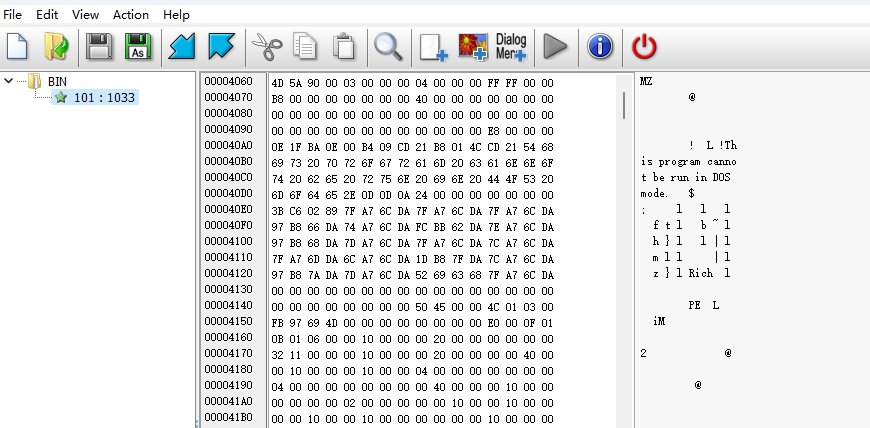


看起来是要向磁盘上写入文件

1. **可以判断\system32\wupdmgrd.exe是否生成**

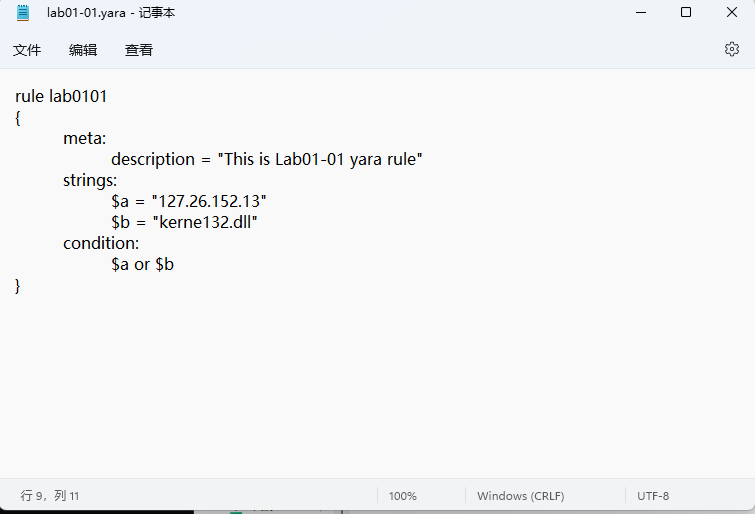
****

1. **发现是一个PE文件**

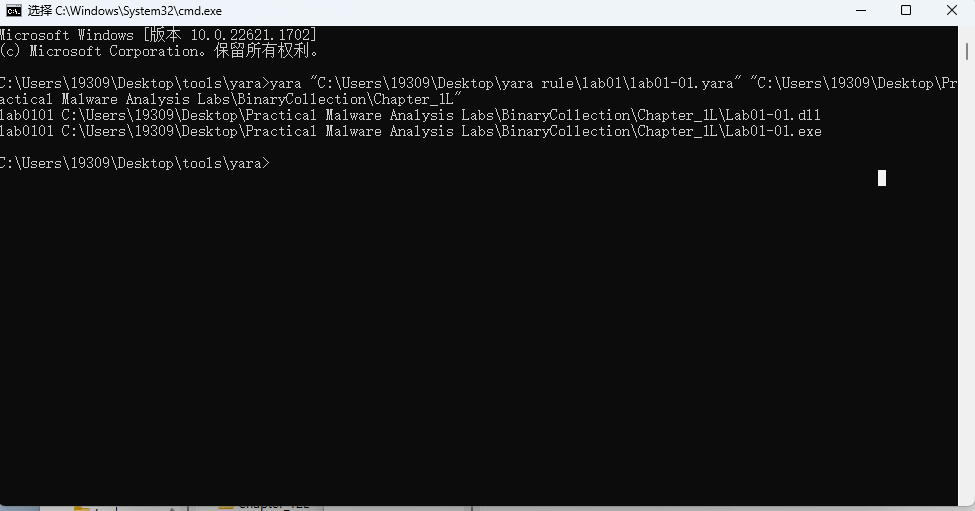


1. **Yara练习**
2. **Lab01-01**

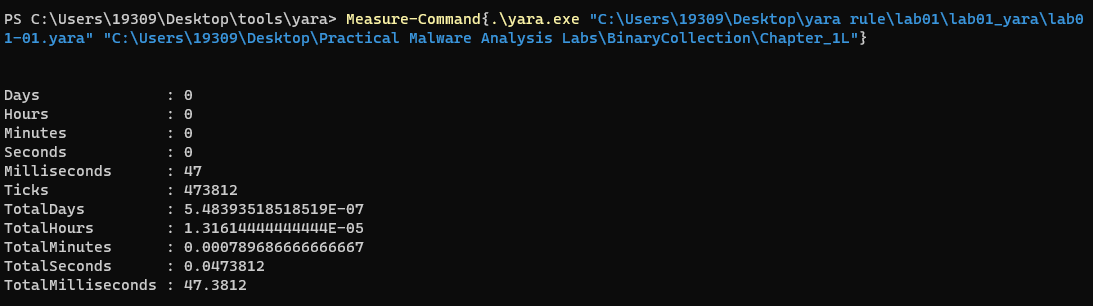
**经调查发现，在.dll文件中存在特殊字符串ipv4地址：127.26.152.13，；而在.exe文件中存在程序意欲创建的特殊文件名称：kerne132.dll。据此可以编写yara规则如下：**



**运行后发现可成功抓取相应的恶意代码**

****

**共执行了47.3812ms**

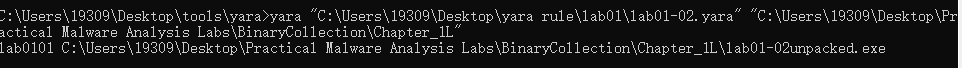


1. **Lab01-02**

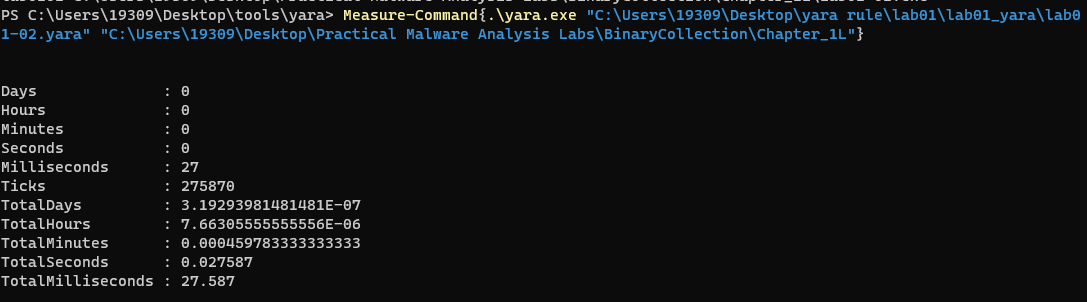
**经脱壳后发现该文件中存在http://www.malwareanalysisbook.com这一特殊网址以及Internet Explorer 8.0这一特殊字符串，据此可以编写yara规则如下：**



**运行后发现可成功抓取相应的恶意代码**

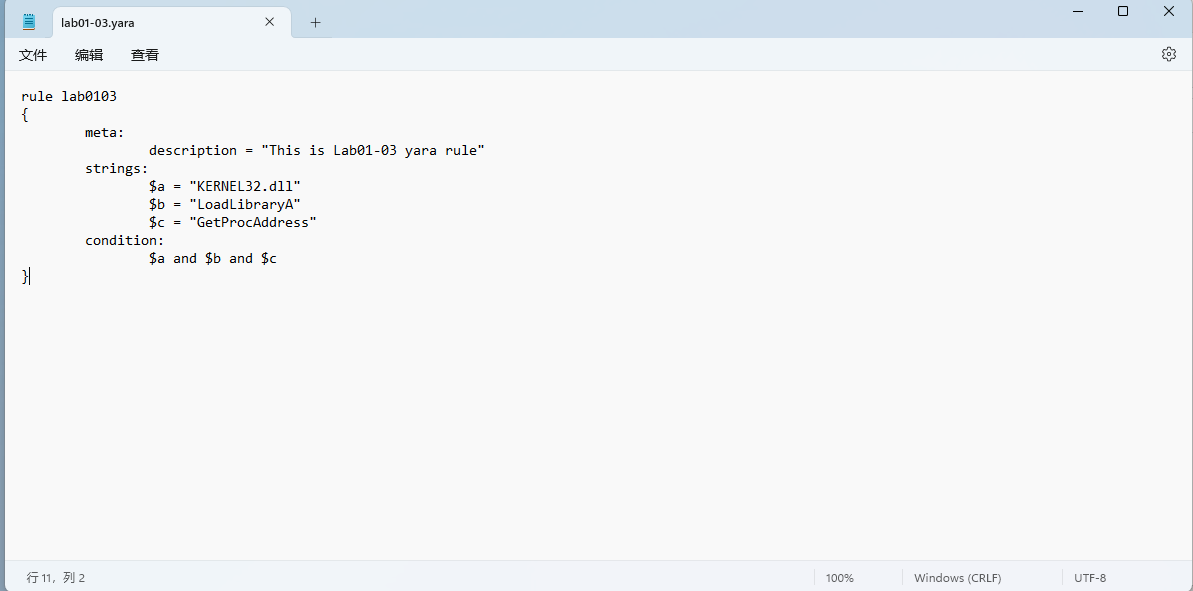


**共执行了27.587ms**

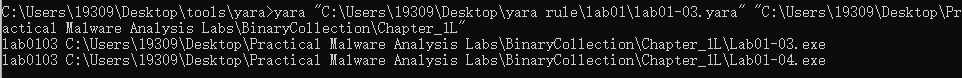


1. **Lab01-03**

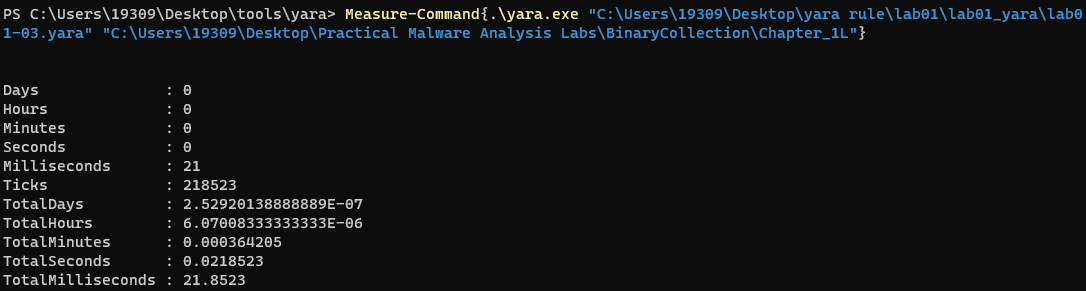
**发现以下特殊字符串：KERNEL32.dll、LoadLibraryA、GetProcAddress。最终构建的yara规则如下：**



**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。**

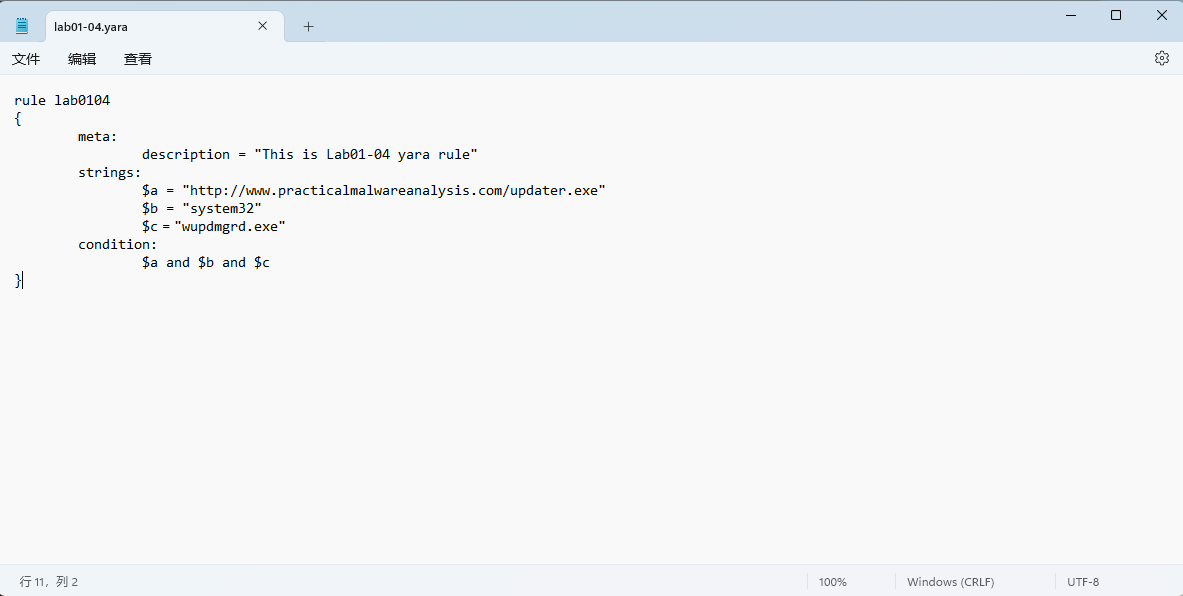


**共执行了21.8523ms**

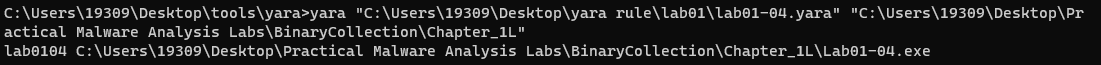


1. **Lab01-04**

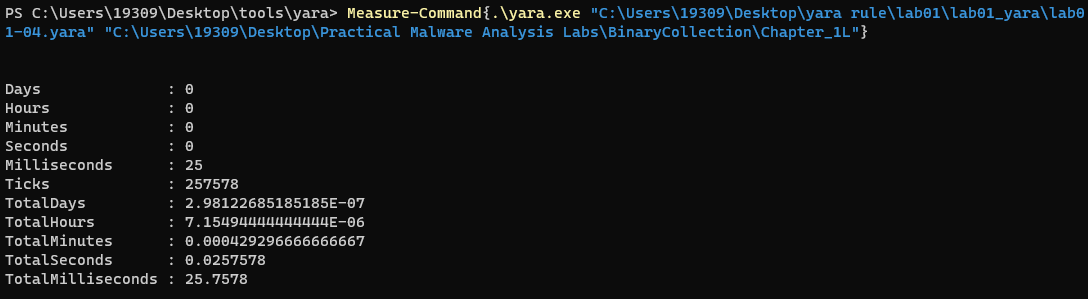
**发现了\system32\wupdmgrd.exe和http://www.practicalmalwareanalysis.com/updater.exe两个特殊字符串。据此构建的yara规则如下：**



**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。**