2023-12-26

北京理工大学计算机学院

计算机病毒防治

实验二 基础动态分析实验报告

目录

[实验准备 3](#_Toc156232043)

[一、 实验环境和所用到的软件 3](#_Toc156232044)

[二、 基本知识 3](#_Toc156232045)

[Lab 3-1 5](#_Toc156232046)

[一、 恶意程序的导入和字符串 5](#_Toc156232047)

[二、 恶意程序在主机上感染的特征 7](#_Toc156232048)

[三、 恶意程序是否有任何有用的基于网络的签名 10](#_Toc156232049)

[Lab 3-2 11](#_Toc156232050)

[一、 如何让这个恶意软件自行安装 11](#_Toc156232051)

[二、 安装后如何运行此恶意软件 14](#_Toc156232052)

[三、 如何找到运行此恶意软件的进程 15](#_Toc156232053)

[四、 为了使用procmon收集信息可以设置哪些过滤器 16](#_Toc156232054)

[五、 恶意软件基于主机的指标是什么 16](#_Toc156232055)

[六、 该恶意软件是否有任何有用的基于网络的签名 17](#_Toc156232056)

[Lab 3-3 17](#_Toc156232057)

[一、 使用Process Explorer监控此恶意软件时注意到什么 17](#_Toc156232058)

[二、 识别任何实时的内存修改 18](#_Toc156232059)

[三、 恶意软件基于主机的指标是什么 19](#_Toc156232060)

[四、 这个程序的目的是 19](#_Toc156232061)

[Lab 3-4 20](#_Toc156232062)

[一、 运行此文件时会发生什么 20](#_Toc156232063)

[二、 导致了动态分析的障碍 21](#_Toc156232064)

[三、 有其他方法运行这个程序吗 22](#_Toc156232065)

[实验总结 23](#_Toc156232066)

# 实验准备

1. 实验环境和所用到的软件

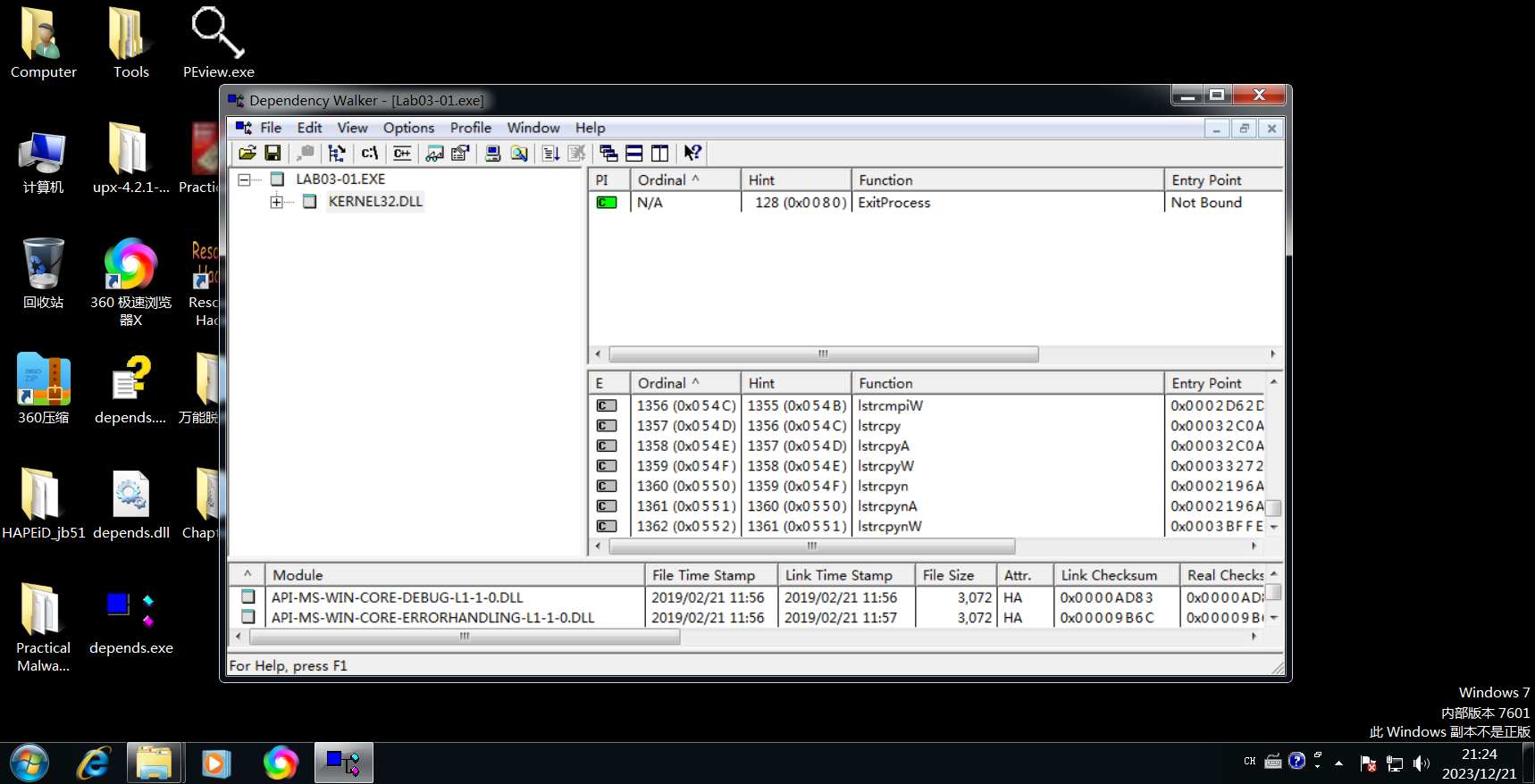
* Windows 7 x64
* rundll32、procmon、Process Explorer、Regshot 、ApateDNS、Wireshark、PE View、Strings等

1. 基本知识
2. 运行恶意DLL
   1. 命令行：rundll32.exe DLL名, 导出参数
   2. 通过改变PE头和扩展名去强迫Windows以EXE方式加载DLL
      1. 擦除在IMAGE\_FILE\_HEADER中的IMAGE\_FILE\_DLL字段
   3. 有些恶意软件需要被安装为一个服务，如Install Service
      1. Rundll32 ipr32x.dll, InstallService ServiceName
      2. Net Start ServiceName
3. 进程监控
   1. Process Monitor：监控注册表、文件系统、网络、进程和线程活动
   2. procmon：即Process Monitor
      1. 实现原理：通过KMonDrv.sys驱动程序
   3. Process Explorer
      1. 验证按钮会验证微软签名
      2. 是否创建了信号量或监听某个端口
      3. 识别进程替换：使用Strings标签页来比较内存中字符串和硬盘上的可执行文件
      4. 右键单击Launch Depends来运行Dependency Walk可以判断DLL是否被加载
      5. 也可以分析恶意文档，如PDFs、Word：先打开Process Explorer，然后再打开恶意文档
4. 创建进程需要调用的函数
   1. CreateProcess
   2. CreateProcessAsUser
   3. CreateProcessWithToken
   4. CreateProcessWidthLogonW
5. 比较注册表项：Regshot
6. 可以创建一个虚假的网络并快速获取网络指标，而无需实际连接到互联网，如DNS、IP、数据包签名
   1. ApateDNS软件
   2. Netcat命令：可以扫描端口的入站和出站信息，隧道，代理和端口转发等等
      1. Nc -l -p 80
   3. Wireshark：可以捕获包和记录网络流量
   4. INETSIM：模拟常见的网络服务
7. 动态分析工具使用
   1. 运行procmon并设置过滤恶意软件名
   2. 启动Process Explorer
   3. 使用Regshot捕获第一个快照
   4. 使用INetSim和ApateDNS创建虚拟网络
   5. 使用Wireshark来记录网络流量

# Lab 3-1

1. 恶意程序的导入和字符串

使用Dependency Walker来查看Lab03-01.exe的导入函数，可以看到只有KERNEL32.DLL中的ExitProcess函数被导入。从结果猜测该文件被加壳了。



使用strings命令来查看Lab03-01.exe的字符串：

文本

描述已自动生成

文本

描述已自动生成

其中一些字符串如域名、WinVMX32、vmx32to64.exe、VideoDriver、还有一些注册表项的键值得我们注意。

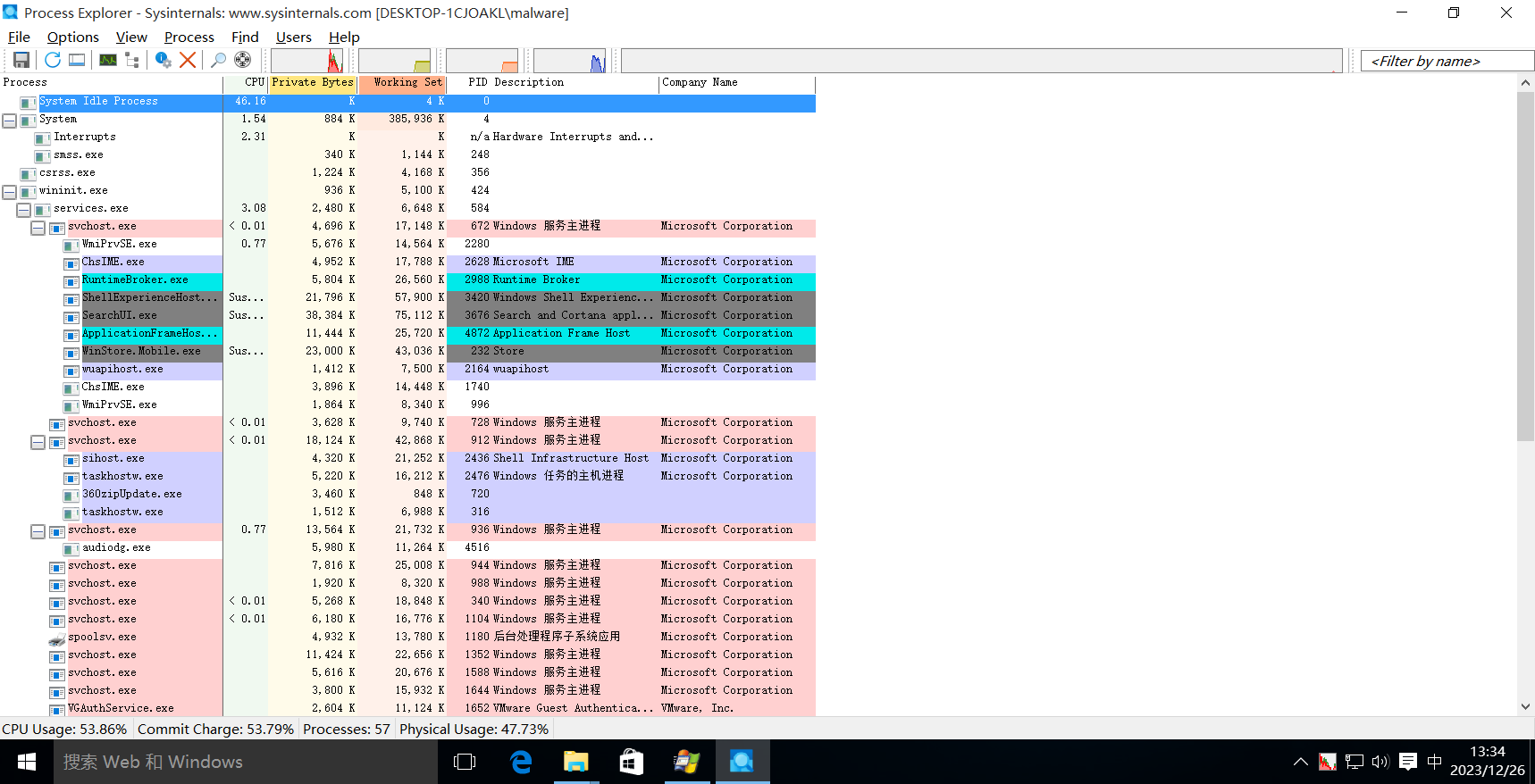
1. 恶意程序在主机上感染的特征

备份恶意程序运行前的注册表。

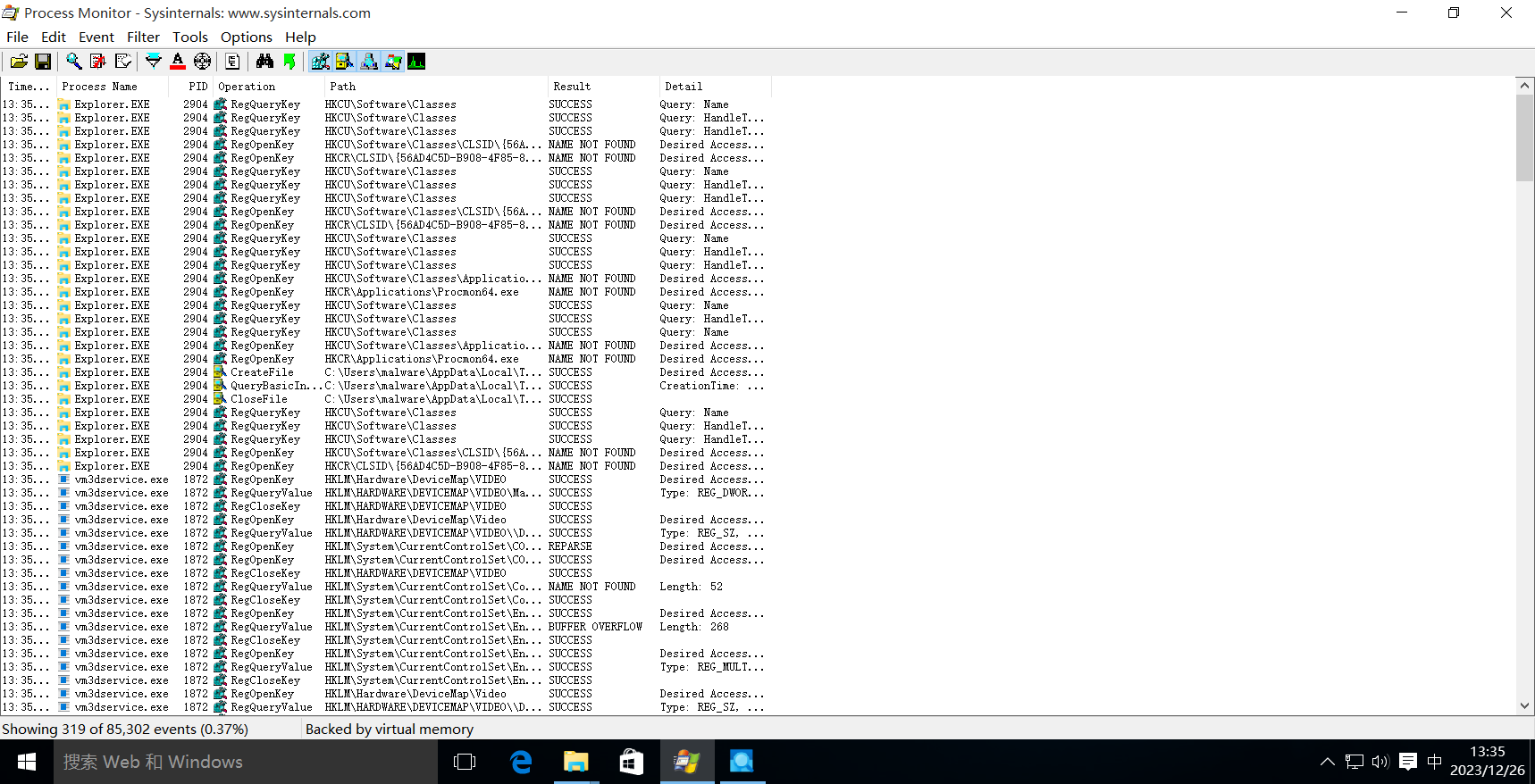
图形用户界面, 应用程序

描述已自动生成

运行Process Explorer。



运行procmon，并清除所有事件。



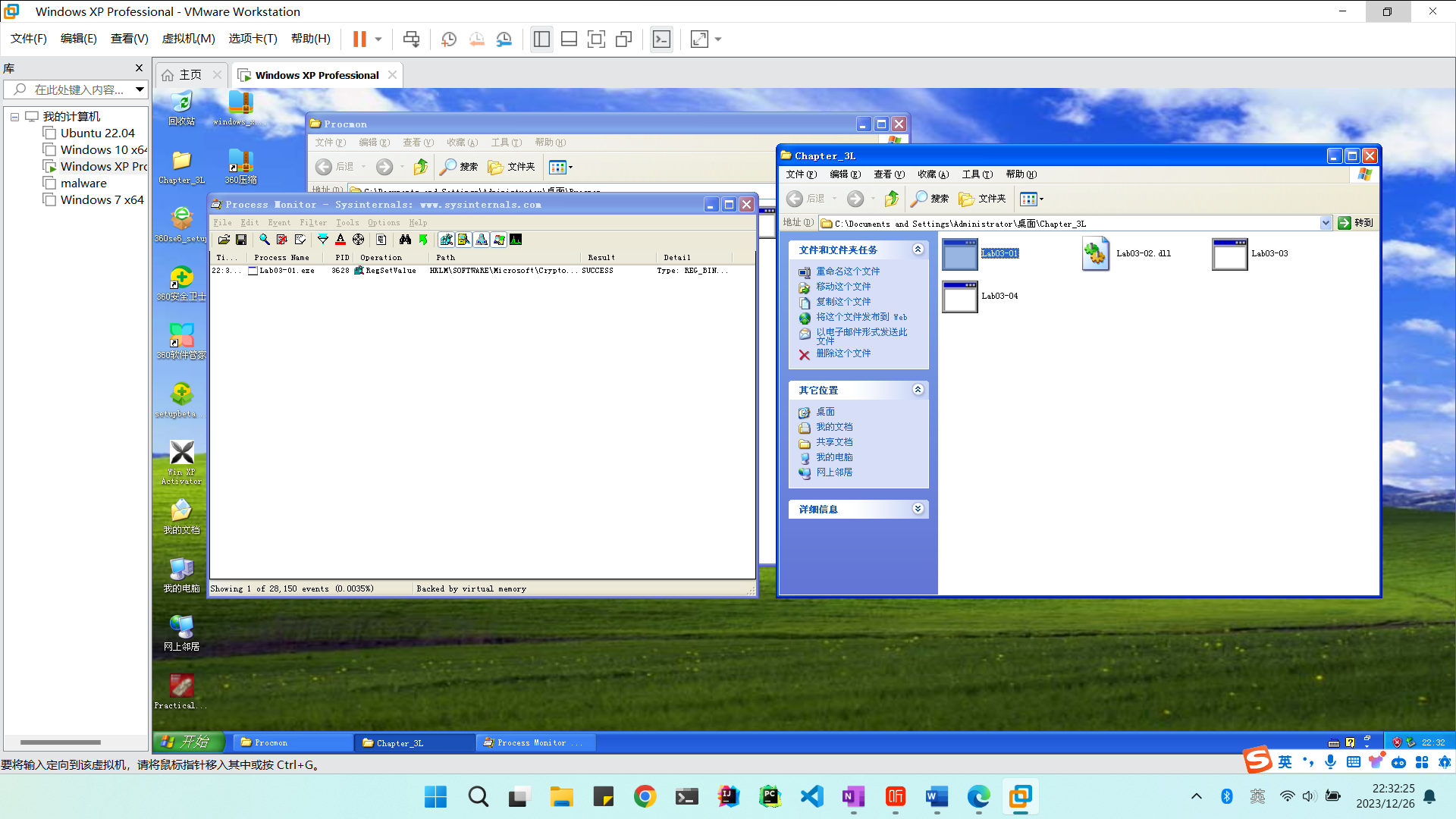
运行Lab03-01.exe恶意程序，但是程序无法启动。

图形用户界面, 应用程序, Word

描述已自动生成

然后我们使用Windows XP来继续分析。

使用Procmon的过滤功能，首先过滤进程名以“Lab”开头，操作为RegSetValue、WriteFile，结果如下：



按照课本上所说，在HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed上调用RegSetValue是典型的噪音，因为随机数生成器种子经常被软件更新注册表。但是没有产生其他事件，所以接下来只能按照课本上所说继续分析了。

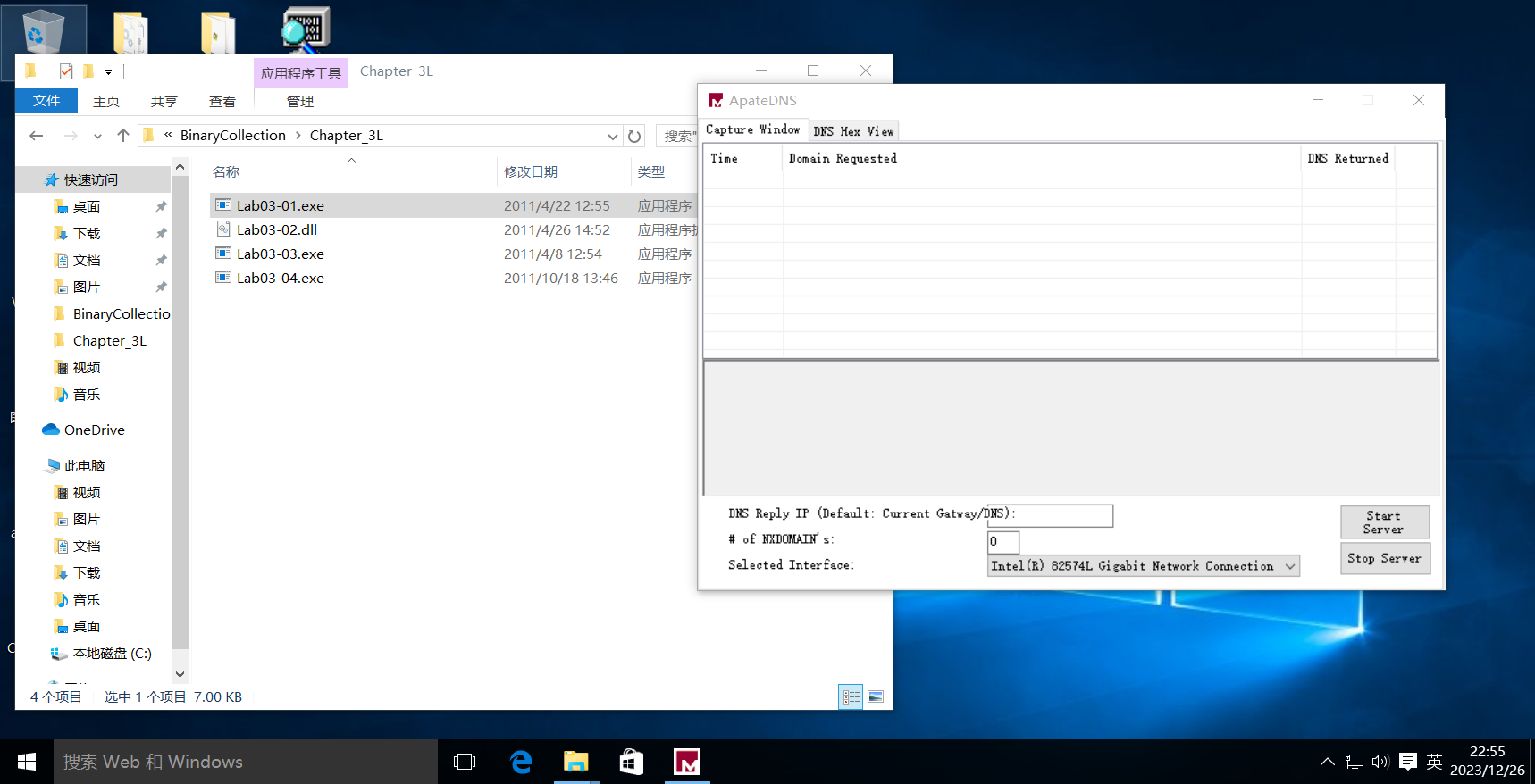
WriteFile操作添加了文件C:\WINDOWS\system32\vmx32to64.exe，且其大小为7178字节，和Lab03-01.exe的大小相等。经过MD5计算发现两个文件是一样的。所以这是恶意软件基于主机的第一个特征。



接下来我们分析对注册表的修改。恶意软件向注册表写入如下值：HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver:C:\WINDOWS\system32\vmx32to64.exe。这表明恶意软件让其开机自启。这是恶意软件基于主机的第二个特征。

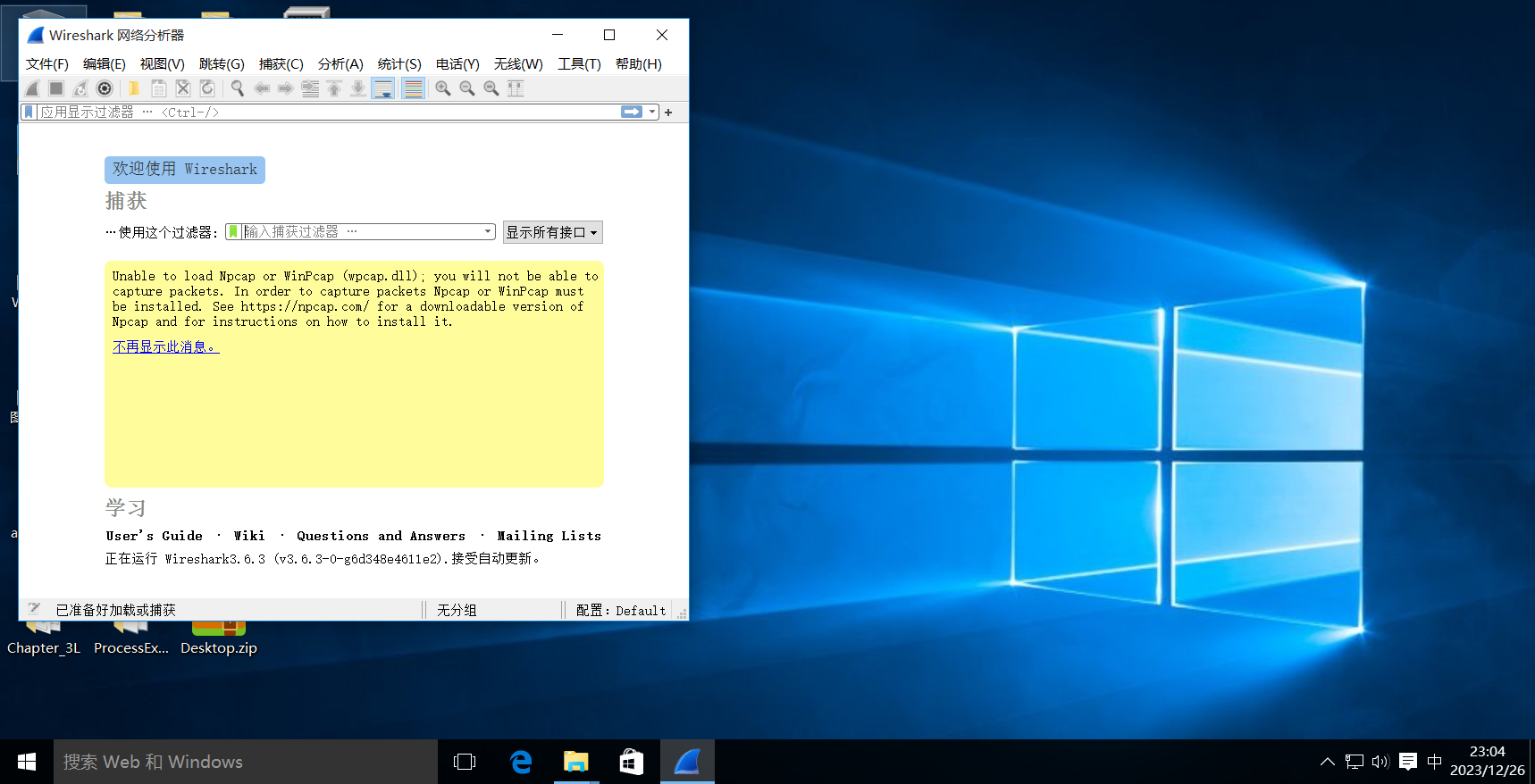
1. 恶意程序是否有任何有用的基于网络的签名

打开ApateDNS软件，然后打开Lab03-01.exe。我们发现恶意软件请求了[www.practicalmalwareanalysis.com](http://www.practicalmalwareanalysis.com)域名。



接下来使用Netcat来检测恶意软件的网络请求。输入命令nc -l -p 443，可以发现控制台输出了一些乱码字符。多次运行此测试发现数据每次似乎都是随机的。可以使用InetSim一次监听所有端口。

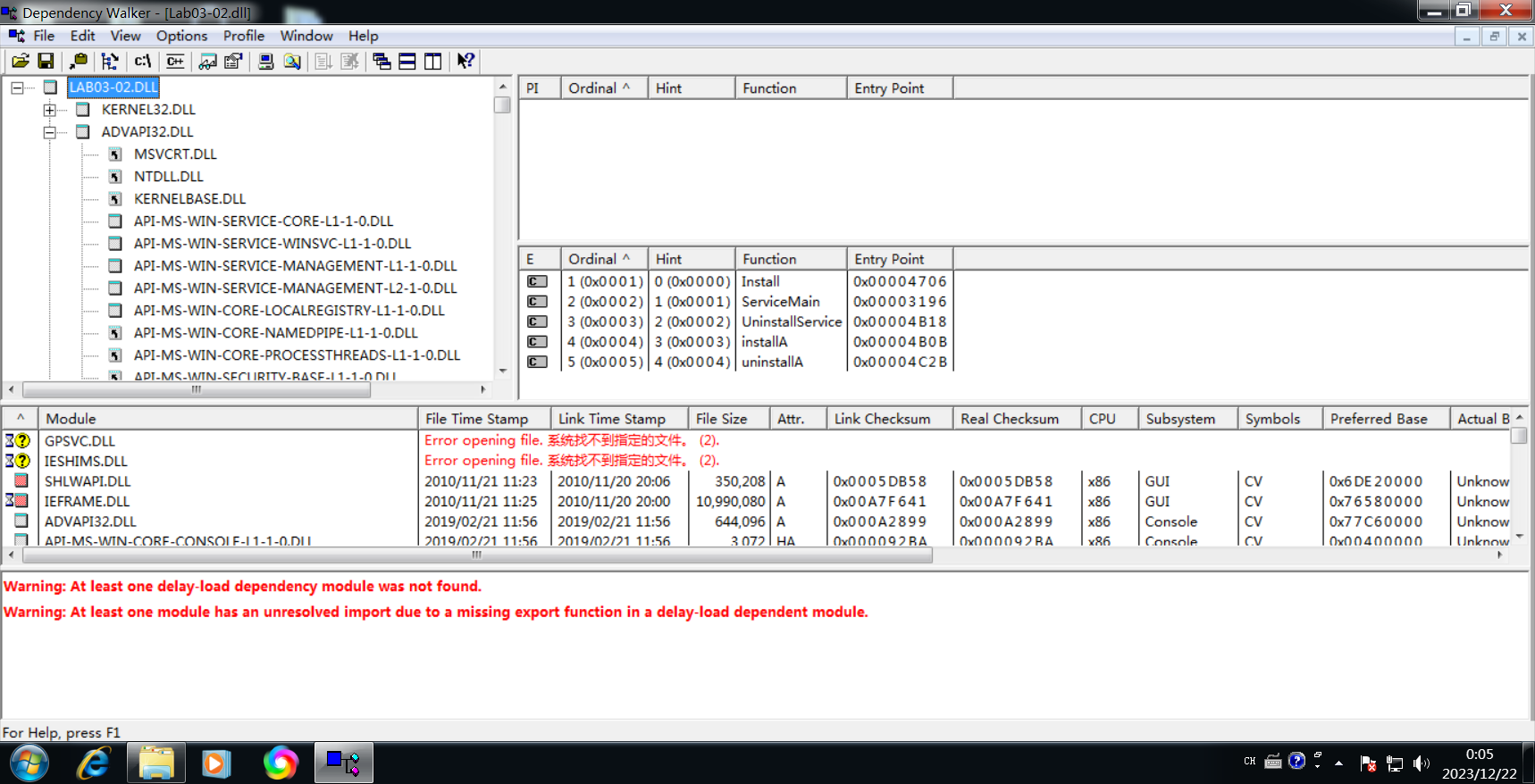
从Wireshark可以得到数据包的大小都是256字节，似乎包含与通常在端口443上运行的SSL协议无关的随机数据。



# Lab 3-2

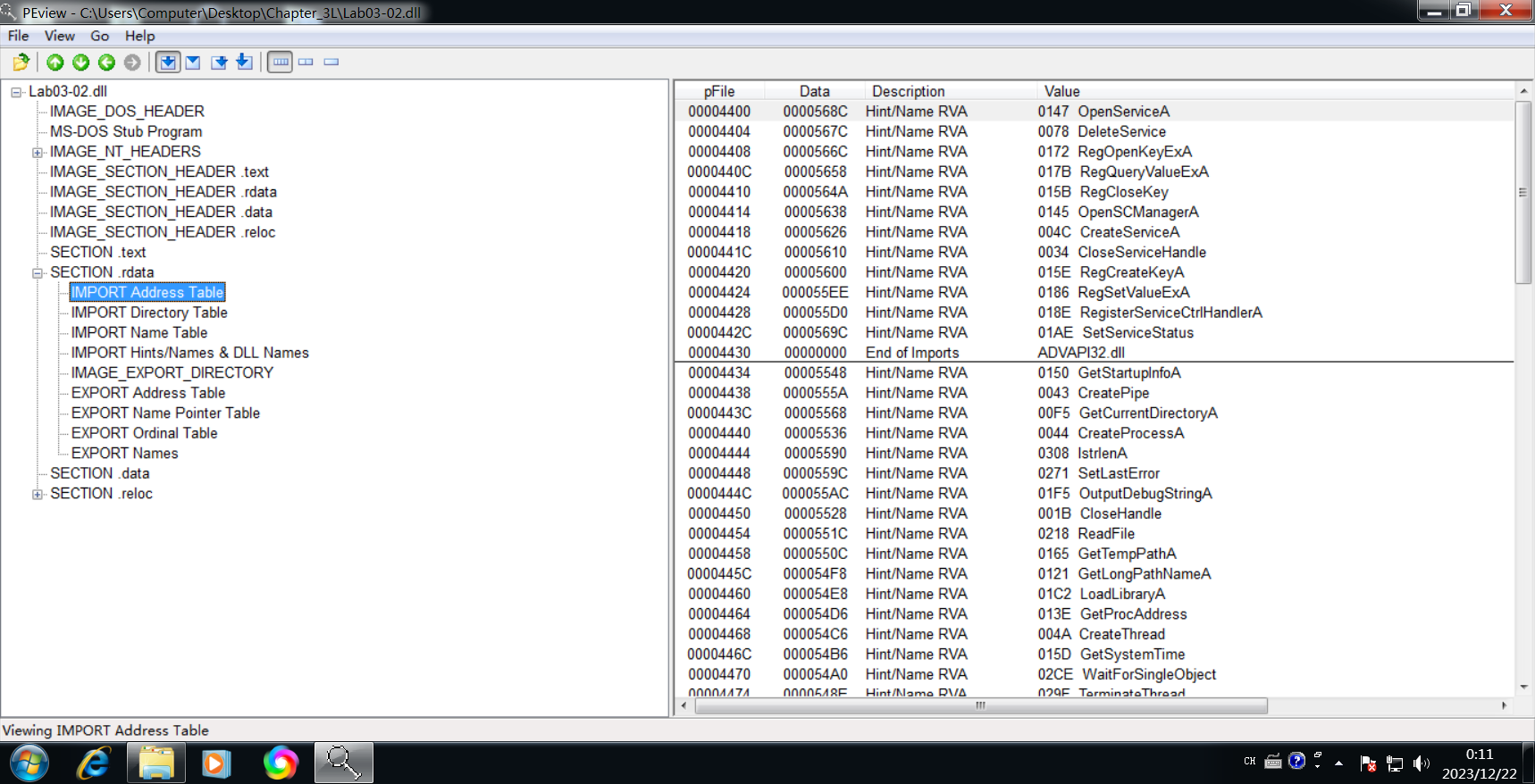
1. 如何让这个恶意软件自行安装

使用Dependency Walker来查看Lab03-02.dll的导出函数，可以发现有Install、ServiceMain、UninstallService、installA、uninstallA这五个函数被导出。



ServiceMain函数暗示该程序需要被安装成服务才能正常运行。

使用PEView来查看程序的导入。



可以看到有与服务操作有关的函数，如CreateService；有与注册表相关的操作的函数，如RegSetValueEx；与网络相关的函数，如HttpSendRequest；创建进程和线程：CreateProcessA和CreateThread。这些暗示该恶意程序使用服务、注册表、HTTP网络服务。

使用strings命令来查看字符串信息。

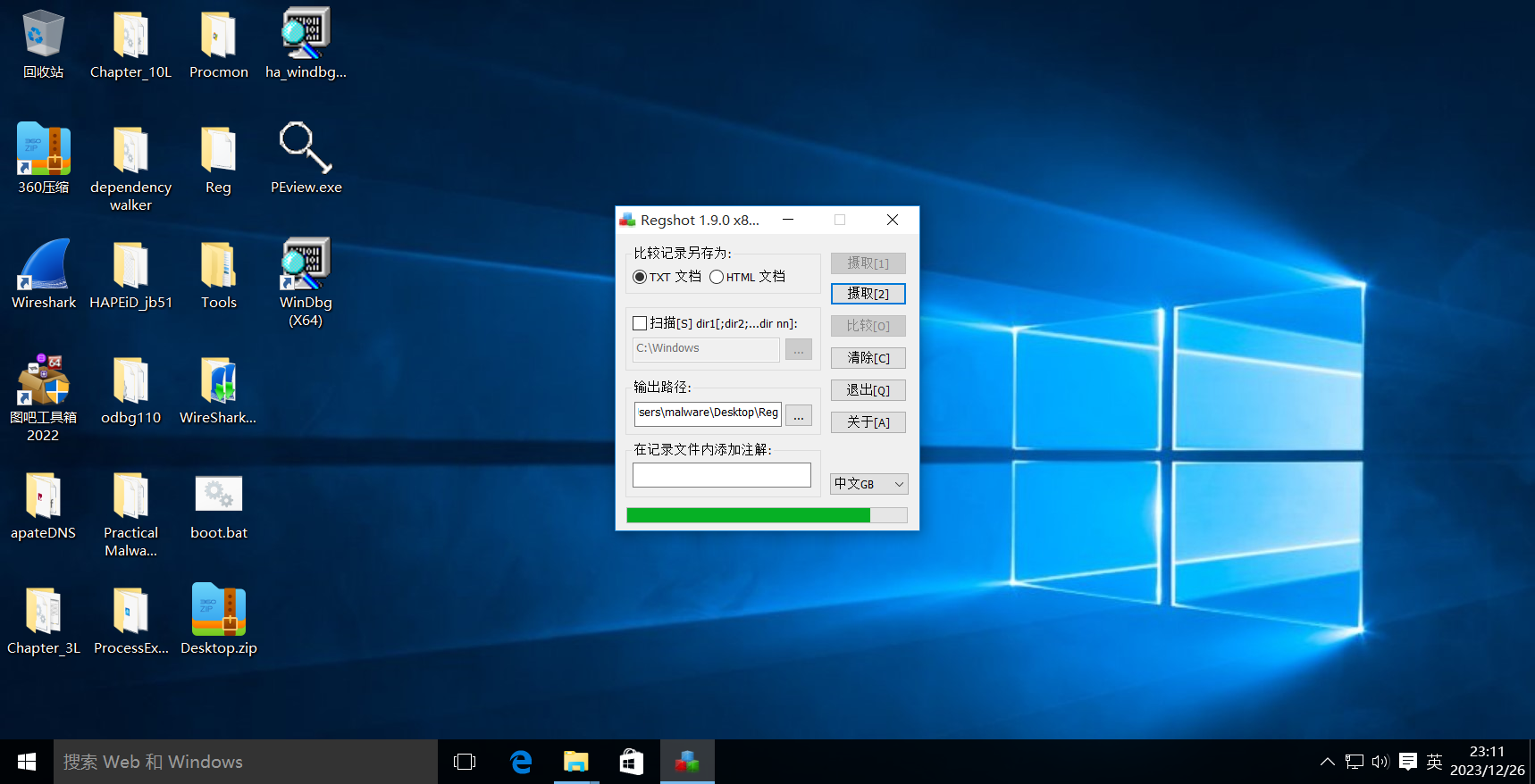
文本

描述已自动生成

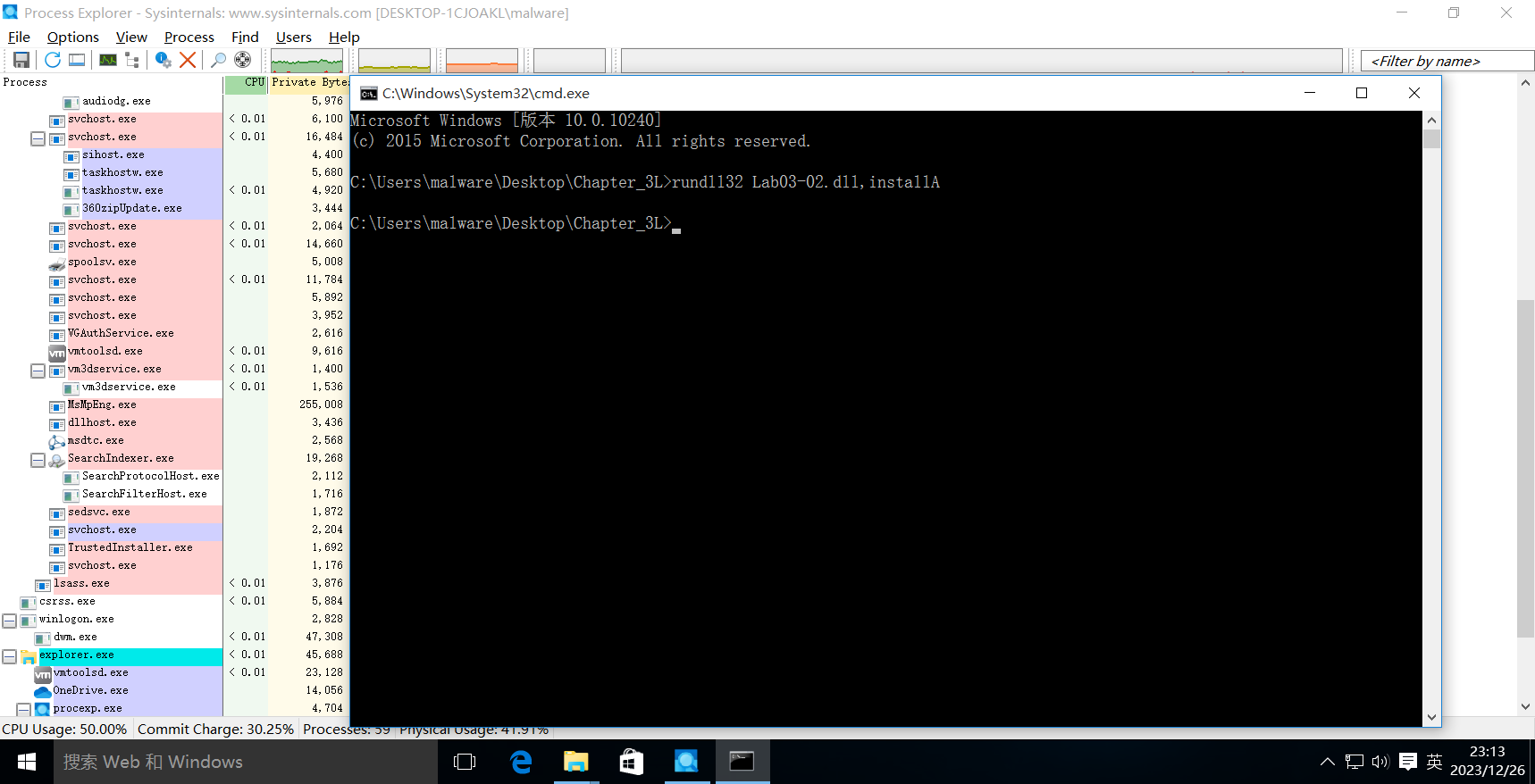
从中可以看到注册表目录：SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost、域名、serve.html、IPRIP、cmd.exe /c表明该程可能会调用cmd.exe创建进程。

以上信息表明，该恶意程序需要通过调用导出函数installA来将安装成为一个服务。

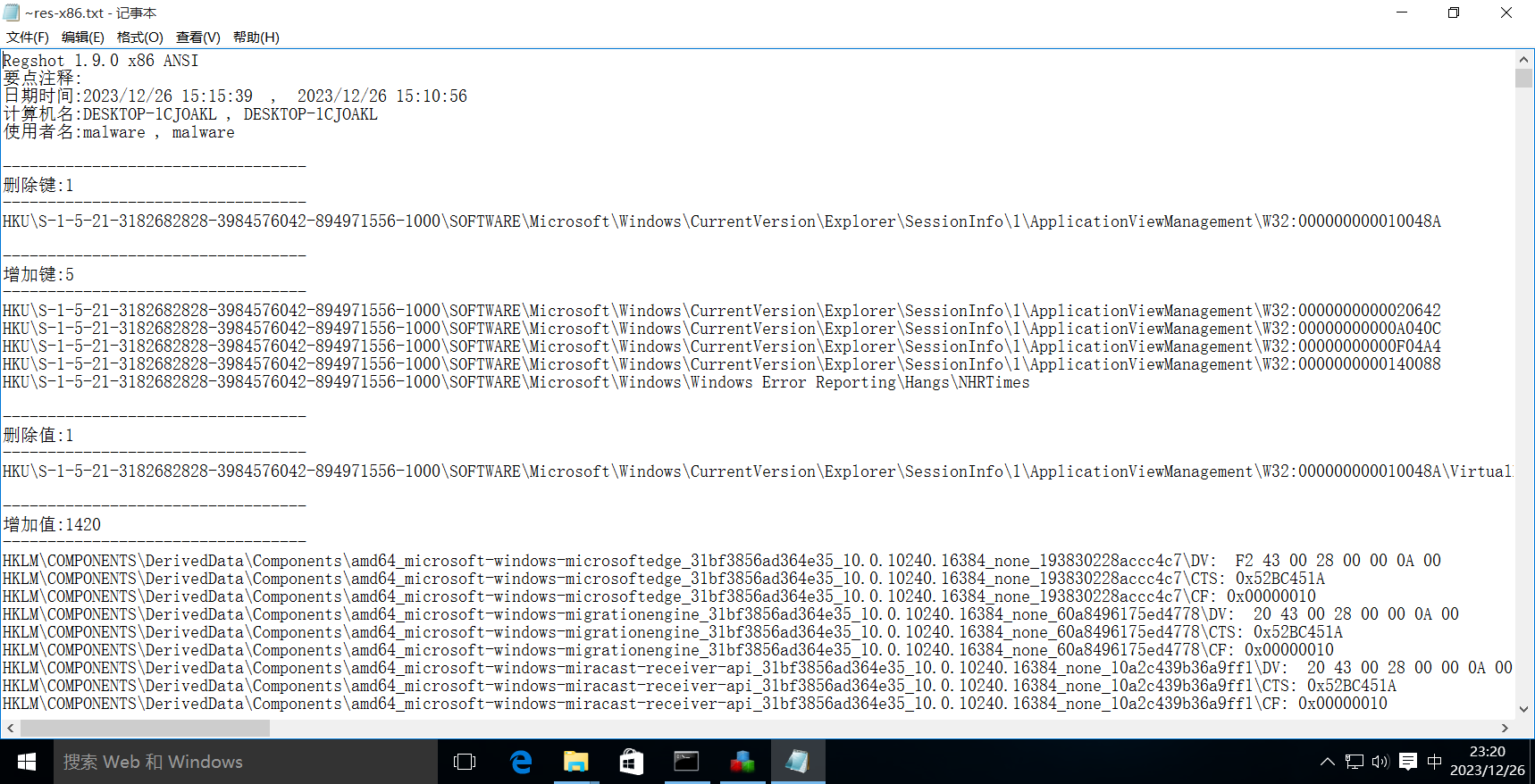
在运行之前，我们使用Regshot来进行注册表的快照，使用Process Explorer来检测运行在程序上的进程。



在命令行中输入C:\>rundll32.exe Lab03-02.dll,installA来安装恶意软件。



使用Process Explorer确保rundll32.exe不在进程列表后，使用Regshot再对注册表进行一次快照，接下来对两次注册表快照进行对比。结果如下：

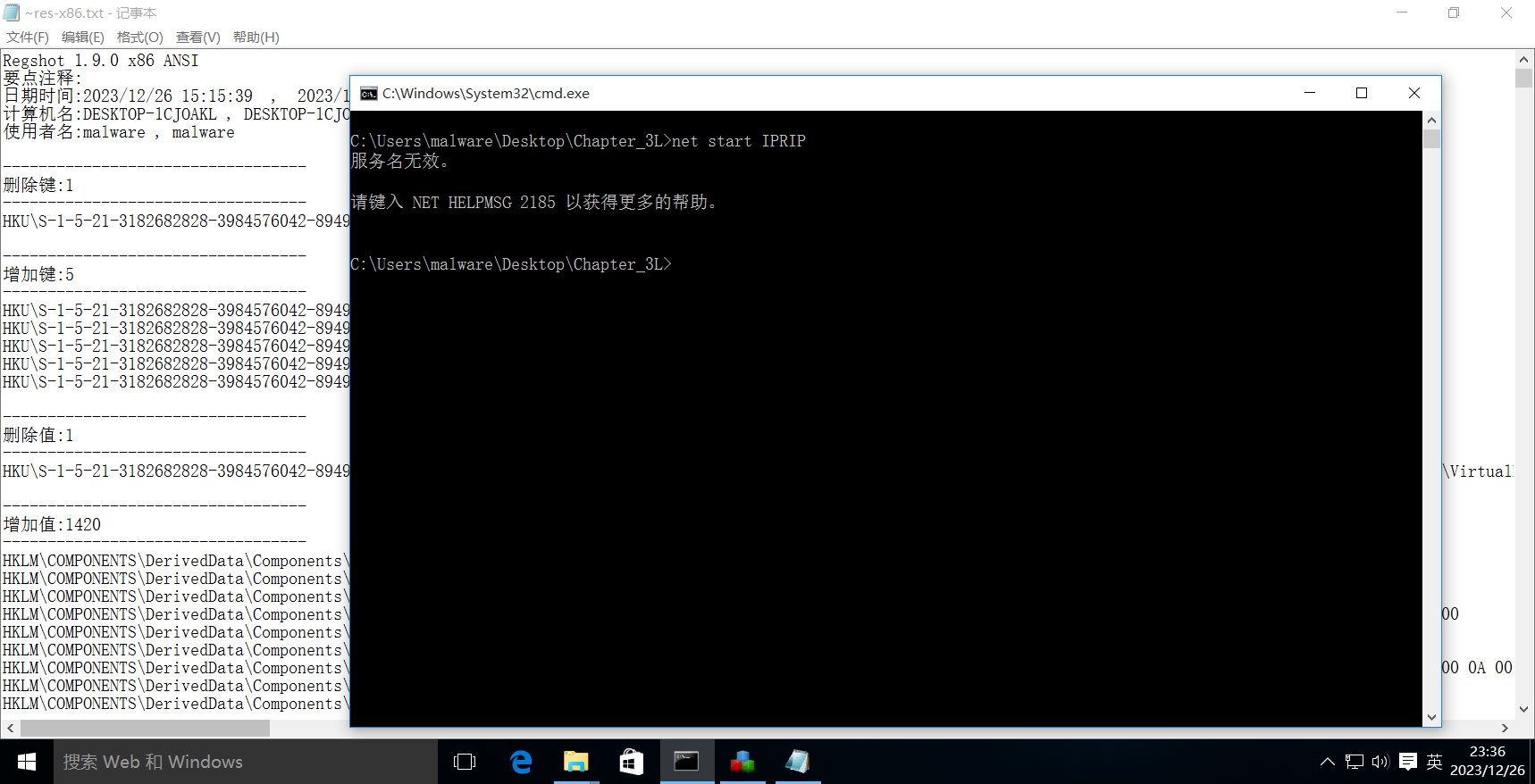


注册表项：HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters\Service Dll表明恶意软件把其安装为IPRIP服务。注册表项：HKLM\SYSTEM\ CurrentControlSet\Services\IPRIP\ImagePath:"%SystemRoot%\System32\svchost.exe -k netsvcs"表明恶意软件将会在svhost.exe进程内启动。剩下的注册表项展现的DisplayName和Description可以作为该恶意软件基于主机的特征。

1. 安装后如何运行此恶意软件

在运行该恶意软件前，我们先启动procmon、Process Explorer、ApateDNS和Netcat监听80端口（因为我们在字符串列表中看到了HTTP）。

因为恶意软件被安装为IPRIP服务，所以接下来我们使用命令net start IPRIP来启动服务。



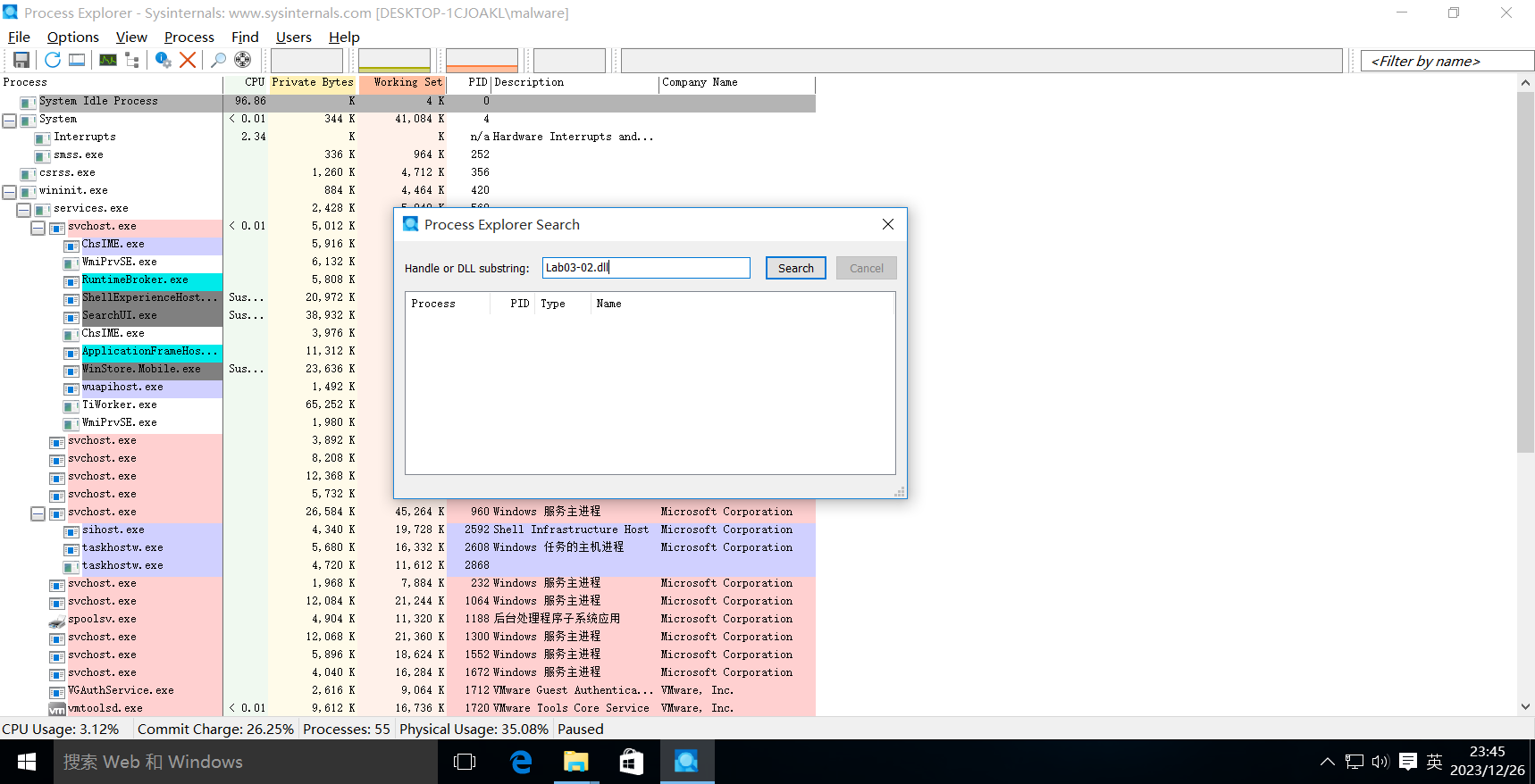
由于该恶意软件无法在我的虚拟机上运行，所以接下来我通过课本答案来继续分析该恶意程序。

按照课本上所说，服务启动后会显示“The Intranet Network Awareness (INA+) service is starting. ”，“The Intranet Network Awareness (INA+) service was started successfully.”。这与之前的注册表项Display的值INA+相匹配。

以上信息表明该恶意软件已经运行了。

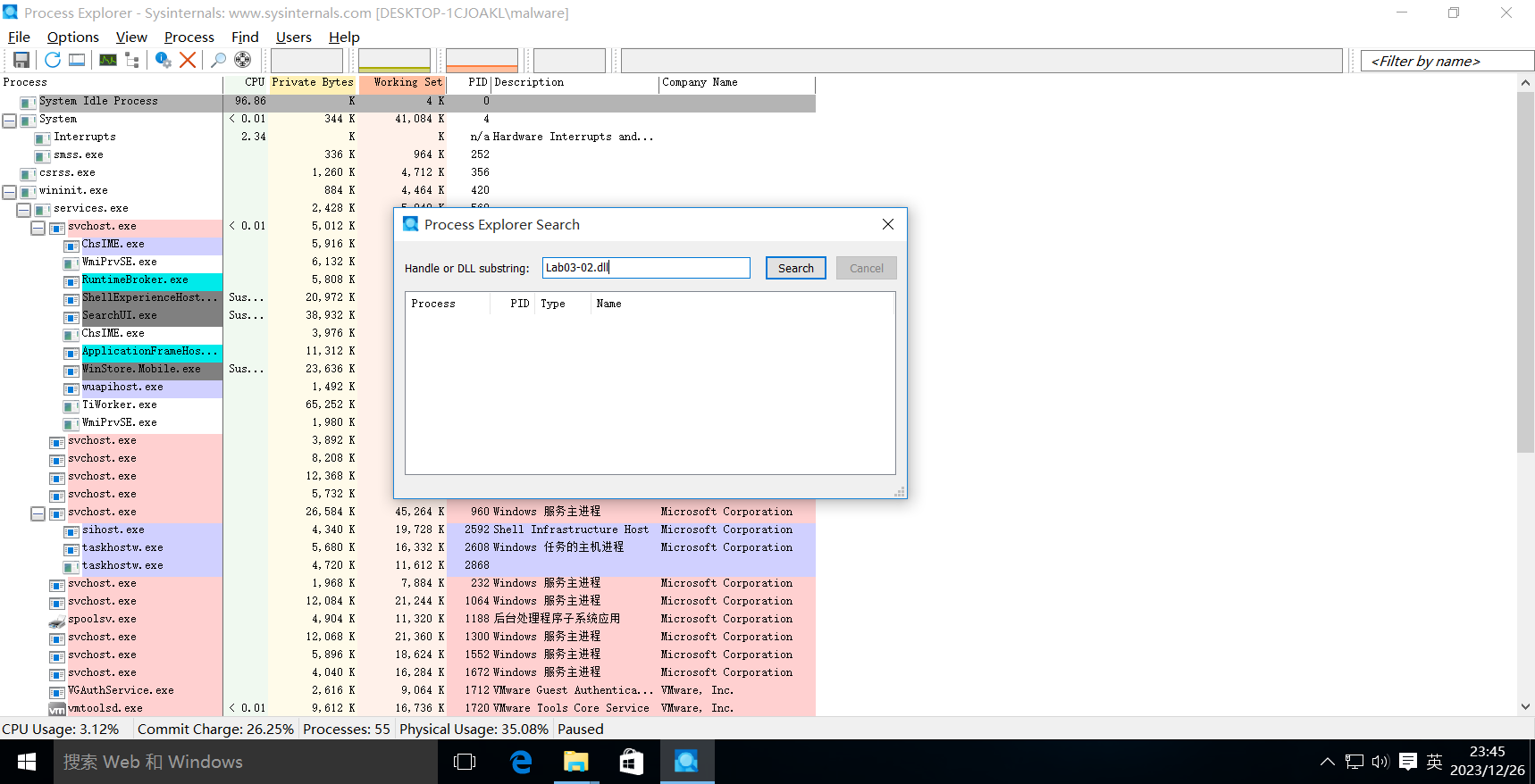
1. 如何找到运行此恶意软件的进程

接下来使用Process Explore来找到运行此恶意软件的进程。选择菜单栏上的Find->Find Handle or DLL，然后输入Lab03-02.dll。



然后我们可以发现svchost.exe加载了Lab03-02.dll。

选择Process Explorer菜单栏上的View->Lower Pane View->DLLs，然后选择svchost.exe进程。



1. 为了使用procmon收集信息可以设置哪些过滤器

可以使用从Process Explorer获取的PID来过滤。

1. 恶意软件基于主机的指标是什么

通过以上分析过程可知：该恶意软件会被安装为服务IPRIP，它的显示名为“Intranet Network Awareness (INA+)”，描述为“Depends INA+, Collects and stores network configuration and location information, and notifies applications when this information changes.”。

其此，该恶意软件会修改注册表：“HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters\ServiceDll: %CurrentDirectory%\Lab03-02.dll”从而实现开机自启。

1. 该恶意软件是否有任何有用的基于网络的签名

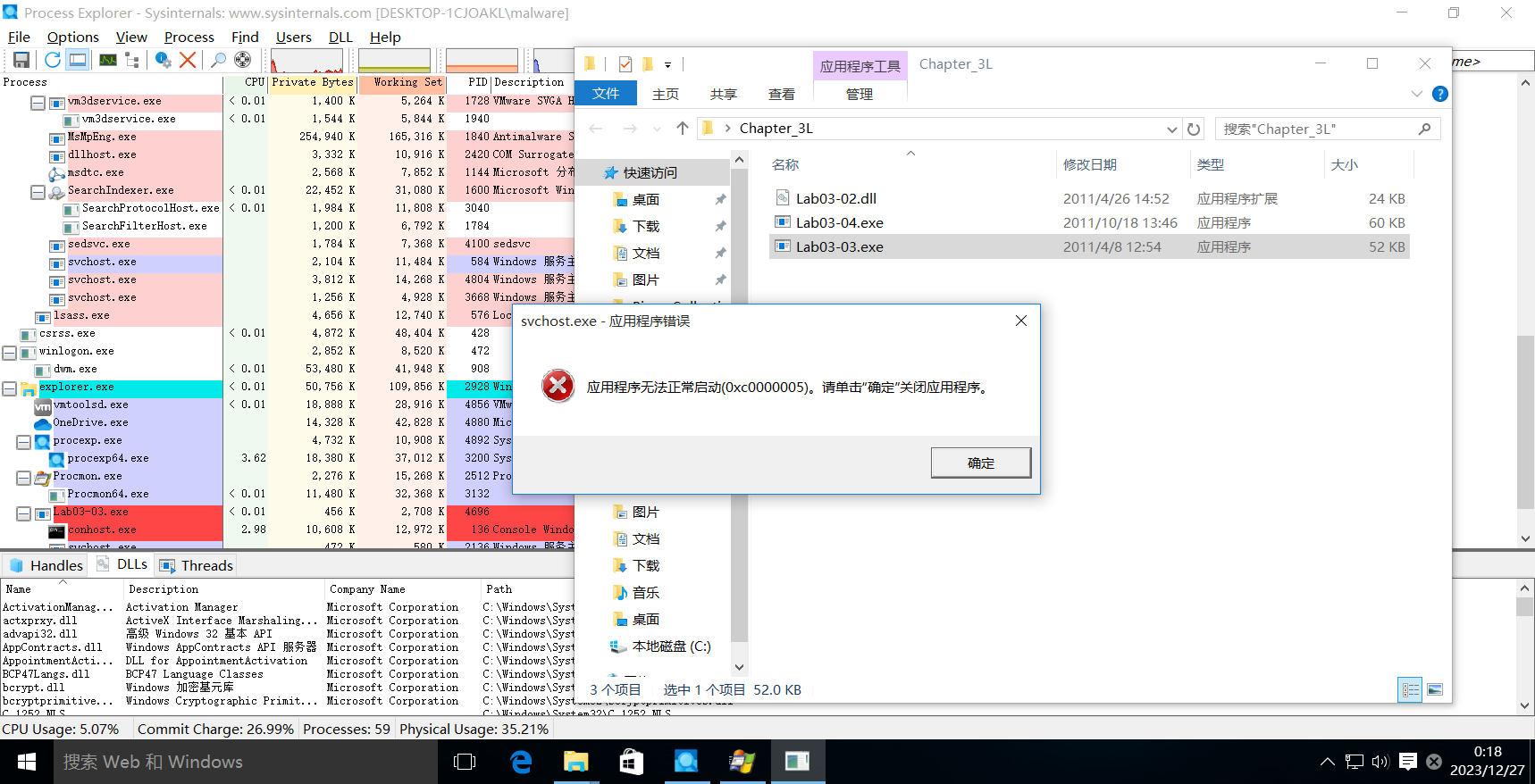
该恶意软件连接到域名practicalmalwareanalysis.com的80端口，并且发起了GET请求来获取serve.html页面，并且User-Agent为%ComputerName%

Windows XP 6.11。

# Lab 3-3

1. 使用Process Explorer监控此恶意软件时注意到什么

打开Process Explorer和procmaon，然后运行Lab03-03.exe。



从上面可以看出，该恶意程序仍然不能在虚拟机中运行。所以我们继续通过分析答案来进行实验。

从Process Explorer中可以看到该恶意程序创建了子进程svchost.exe，然后退出，svchost.exe成为了孤儿进程。

一般情况下，svchost.exe是services.exe的子进程。所以这个孤儿进程就很值得怀疑。

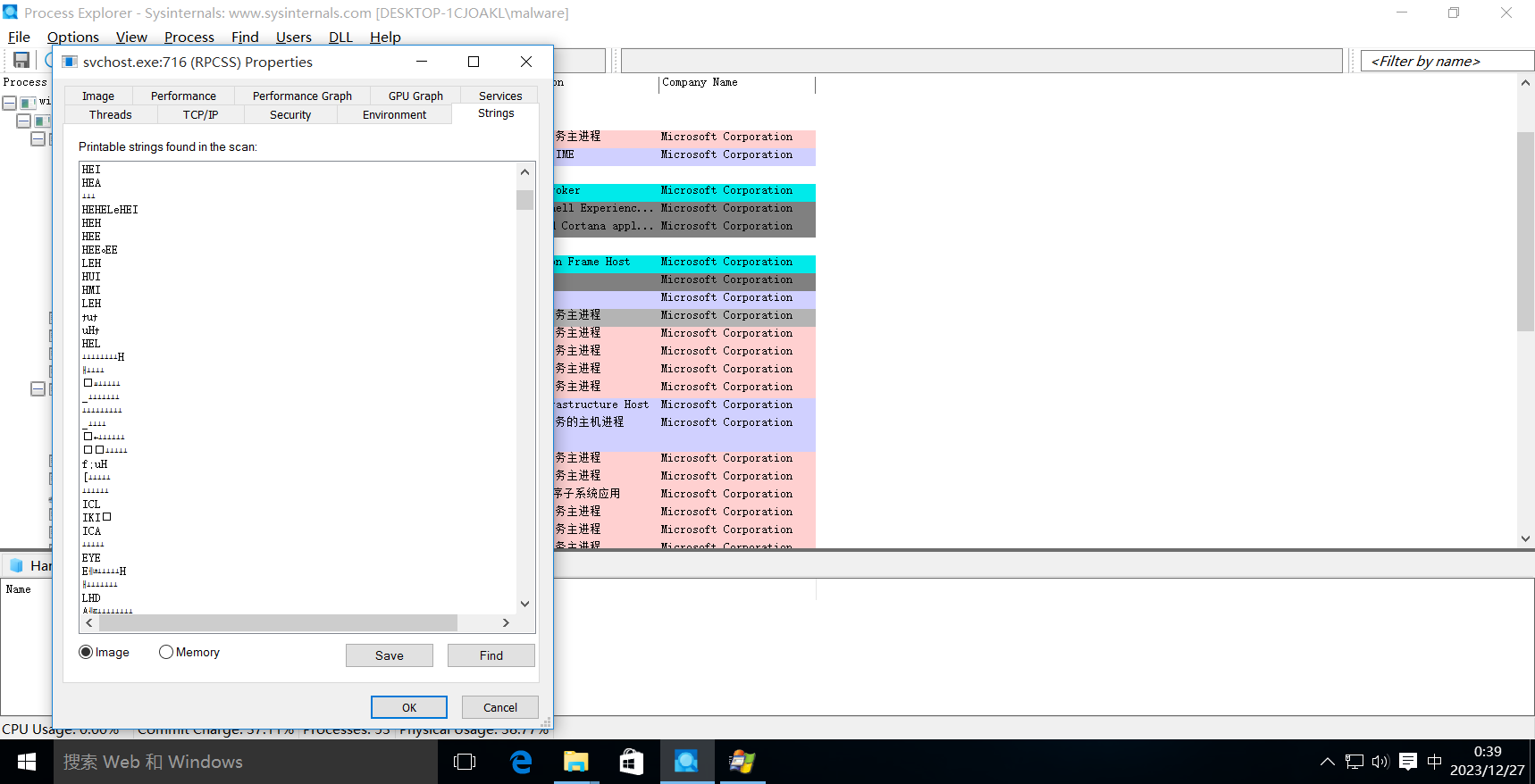
1. 识别任何实时的内存修改

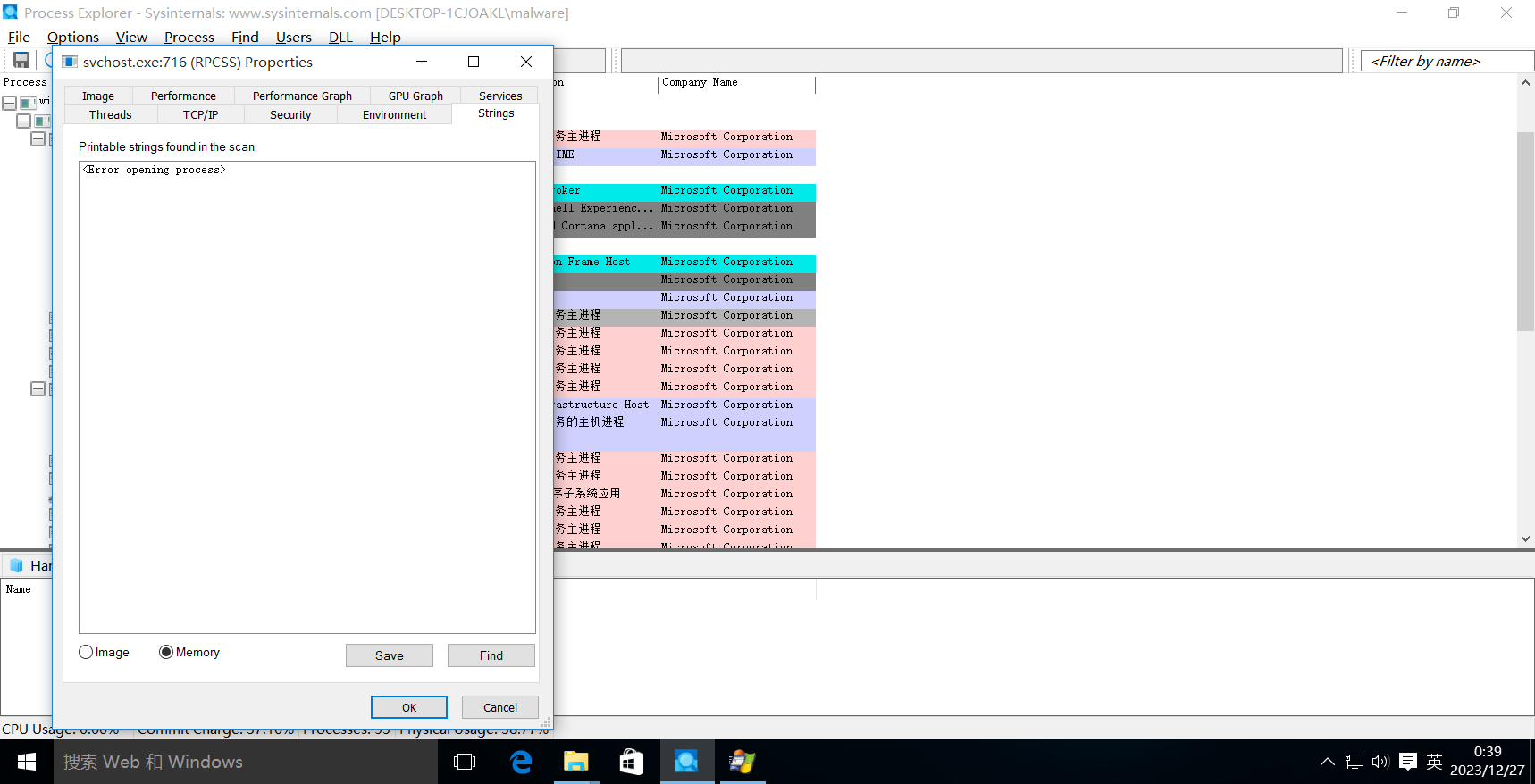
在Process Explorer选中孤儿进程svchost.exe，并右键点击Properties打开该进程的属性窗口。

图形用户界面, 文本, 应用程序

描述已自动生成

选中Strings子标签栏来显示文件和内存中字符串。可以发现在内存中的字符串多了“practicalmalwareanalysis.log”、“[ENTER]”。





1. 恶意软件基于主机的指标是什么

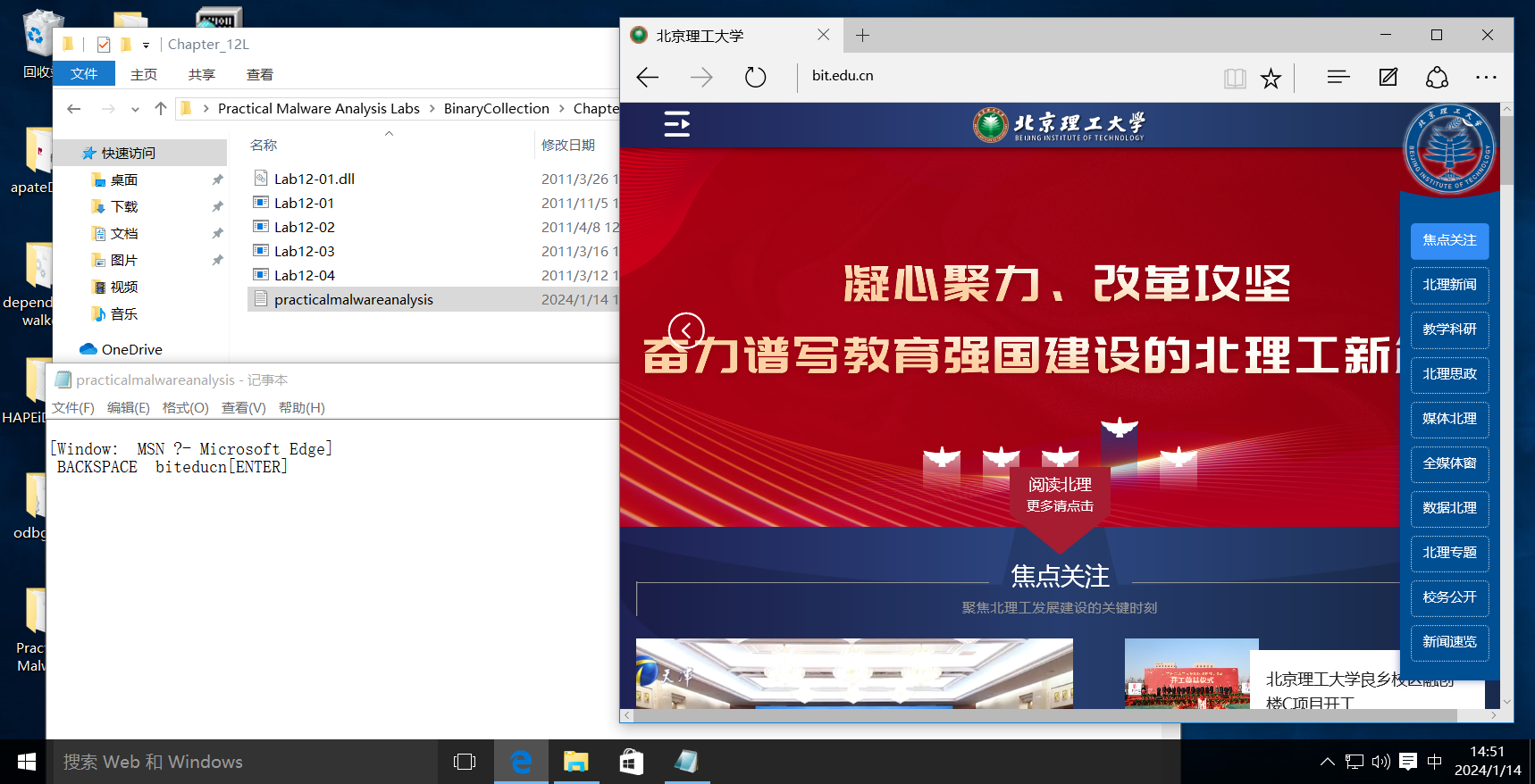
该恶意软件创建了名为practicalmalwareanalysis.log的文件。

1. 这个程序的目的是

字符串“practicalmalwareanalysis.log”、“[ENTER]”、“[CAPS LOCK]”的存在表明该软件可能是一个键盘记录器。

为了检验我们的猜测，我们可以在记事本中输入一段字符。然后使用Procmon并设置过滤条件为孤儿进程的PID来获取该恶意软件的事件。然后发现有CreateFile和WriteFile事件并写入了文件名为practicalmalwareanalysis.log的文件。

检查practicalmalwareanalysis.log文件的内容，发现其中的内容和我们刚才的输入相同。

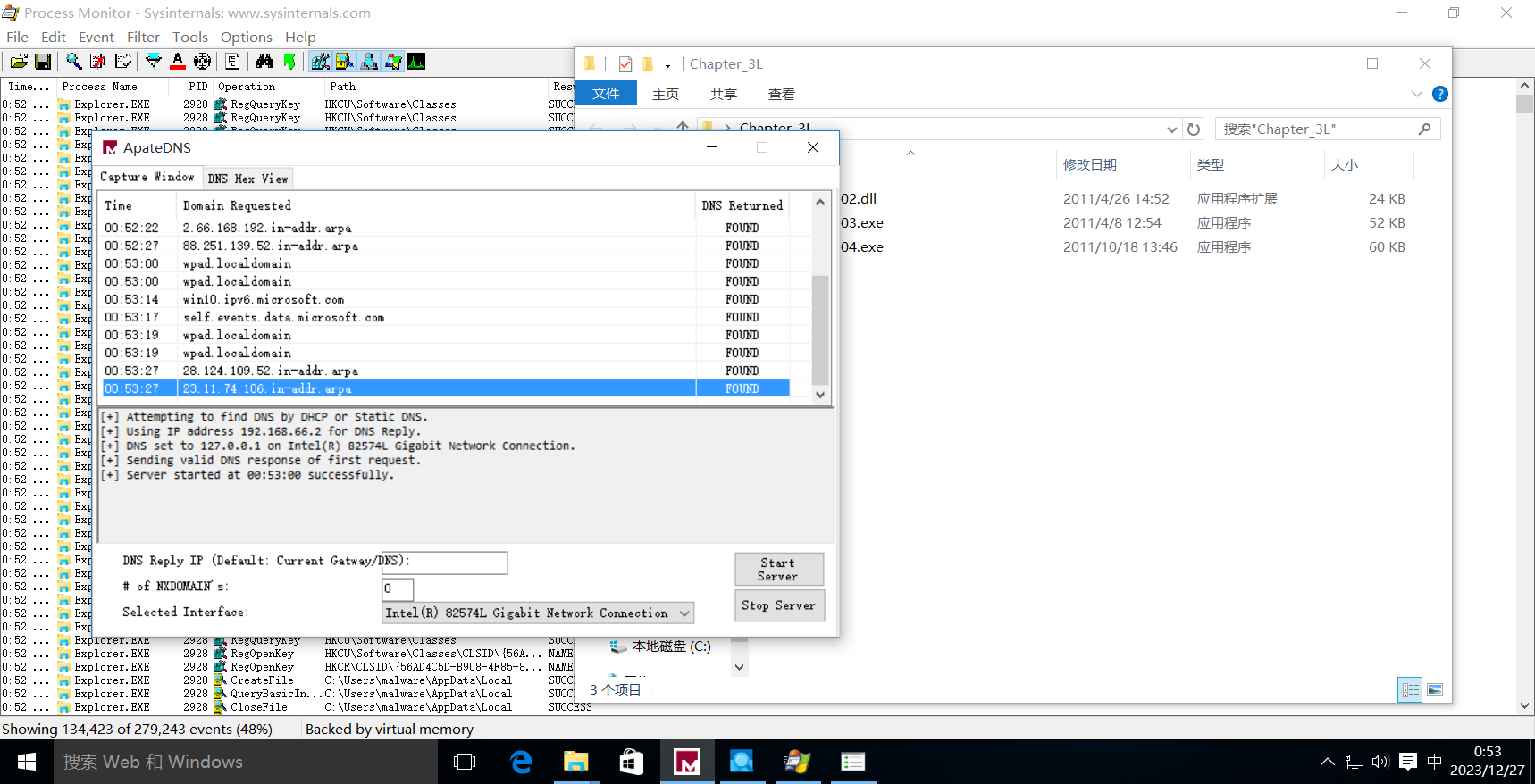


综上，该软件是一个使用进程替换的键盘记录器。

# Lab 3-4

1. 运行此文件时会发生什么

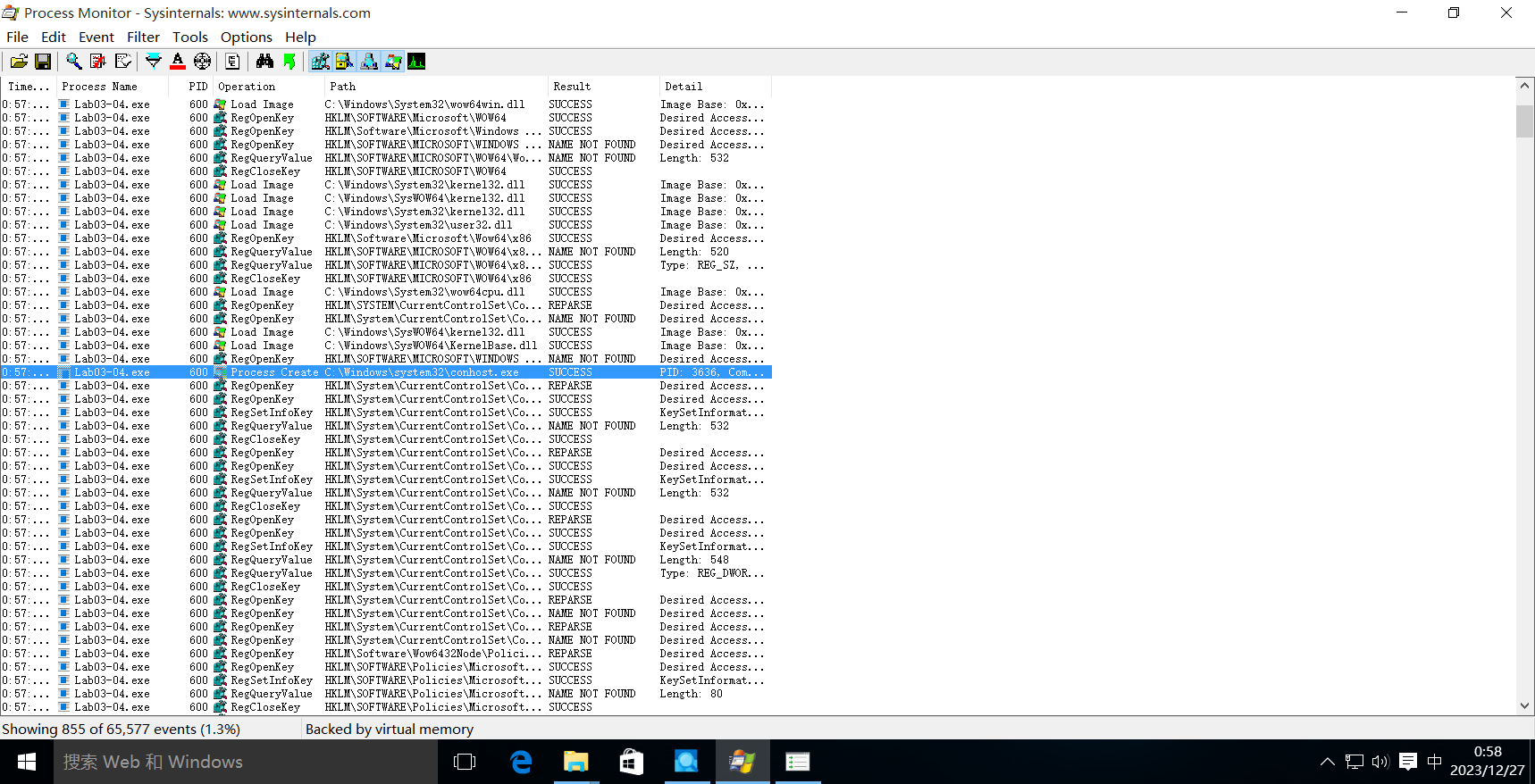
打开procmon和Process Explorer，并设置虚拟网络。然后运行Lab03-04.exe。结果如下。



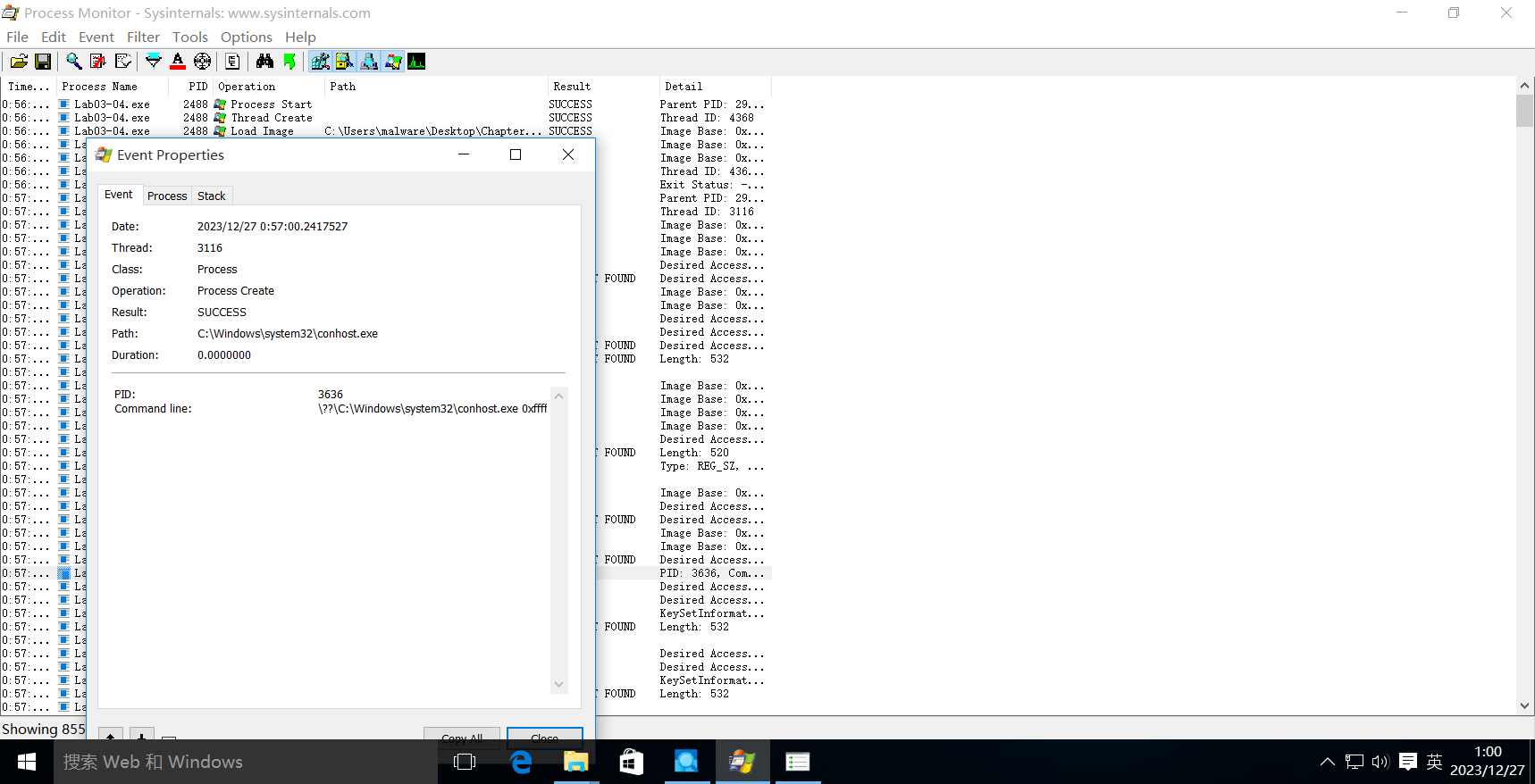
当运行这个程序时，该恶意程序立即删除自己，并且在Process Explorer也看不到其他有用的信息。

1. 导致了动态分析的障碍

接下来，我们使用Procmon，并设置进程名为Lab03-03.exe的过滤，结果如下：



我们发现了Process Create项，双击可以看到它的命令行。我们可以发先它正在调用“C:\WINDOWS\system32\cmd.exe" /c del Z:\ Lab03-04.exe >> NUL”来删除自己。



经过以上分析，我们可以猜测该软件可以需要一些参数，也可以缺少一些组件。

1. 有其他方法运行这个程序吗

我们可以尝试通过strings命令找到的形如命令行参数的字符串，如“-in”、“-re”、“-cc”、“-c”。但是经过尝试该程序仍然会删除自己。

图形用户界面, 应用程序

描述已自动生成

# 实验总结

本次实验，让我认识到了一些基本动态分析工具的使用，这其中我觉得最为强大的是procmon，它可以检测进程运行后各种操作和事件。其次，一些网络分析工具对实验也很有帮助，但是由于环境的限制，我对某些工具没有进行实际使用。虽然Windows XP可以运行所有恶意软件，但是不知道什么原因Windows XP在我的虚拟机上运行非常卡顿，之后我会更换其他类型的操作系统的虚拟机进行之后的实验。