个人信息

学号：1911410

姓名：付文轩

专业：信息安全

lab 3-1

要求

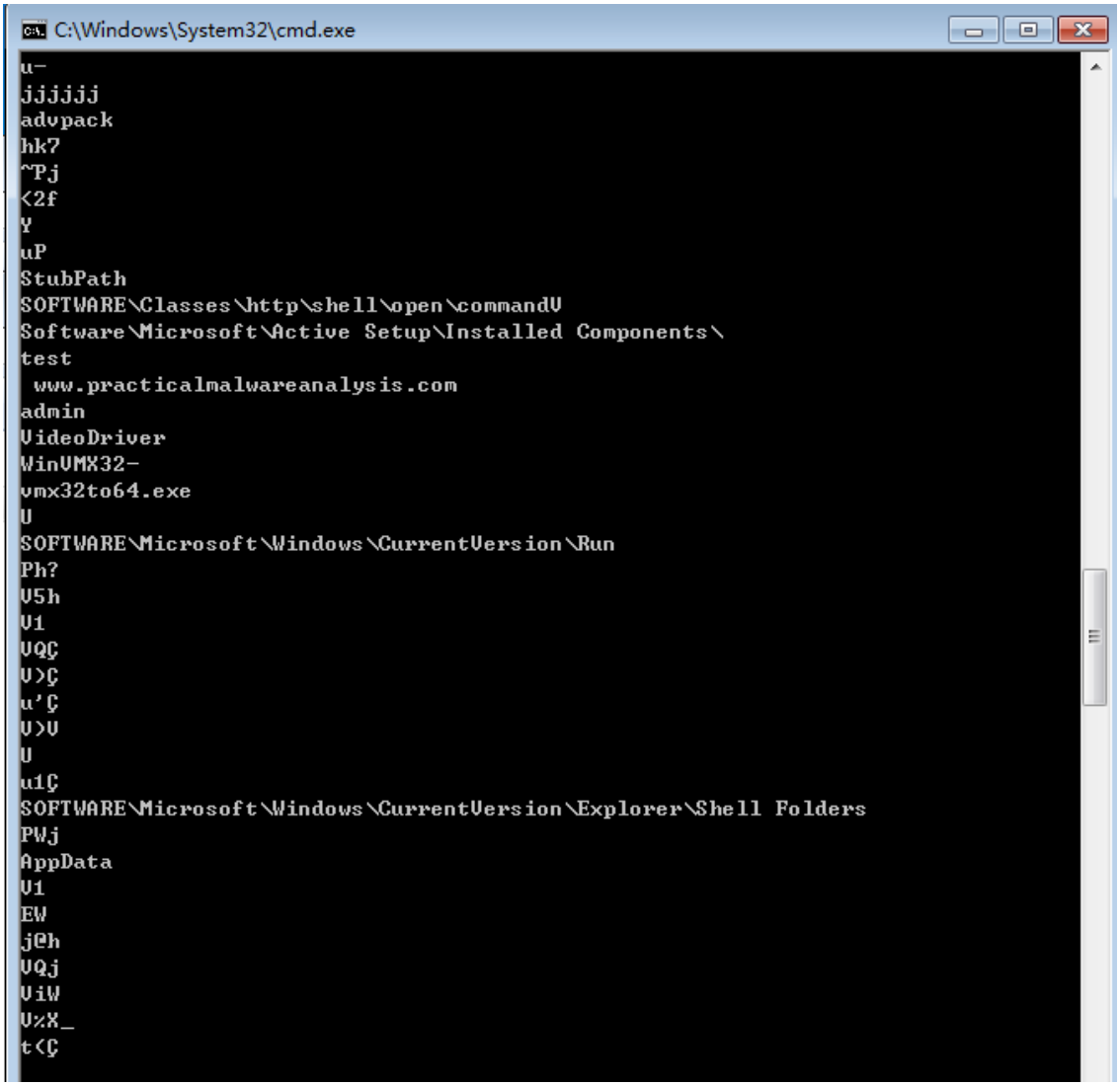
Analyze the malware found in the file *Lab03-01.exe* using basic dynamic analysis tools.

Questions

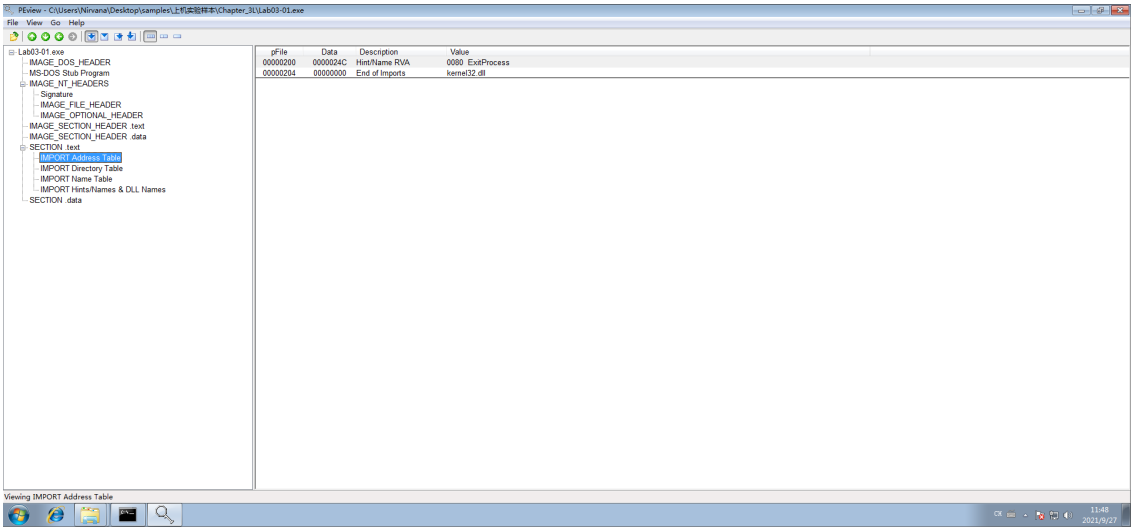
1. What are this malware's imports and strings?
2. What are the malware's host-based indicators?
3. Are there any useful network-based signatures for this malware? If so, what are they?

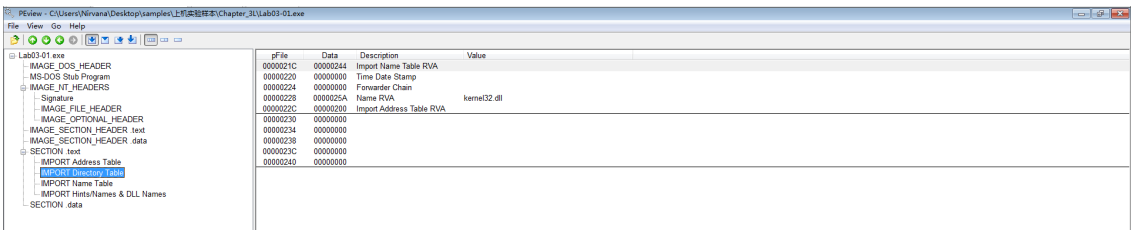
实验过程

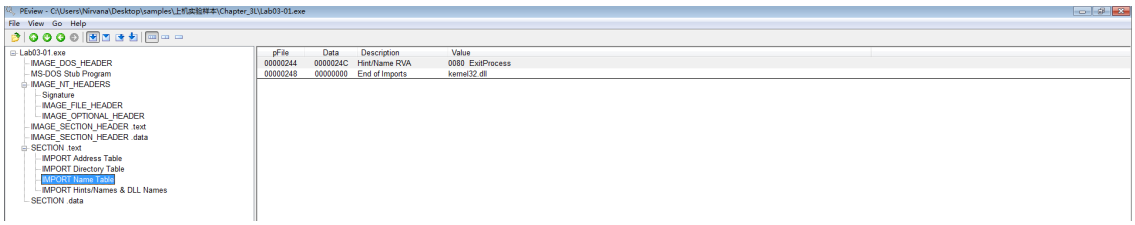
1. 首先使用Strings工具扫描lab03-01.exe，得到结果如下图：

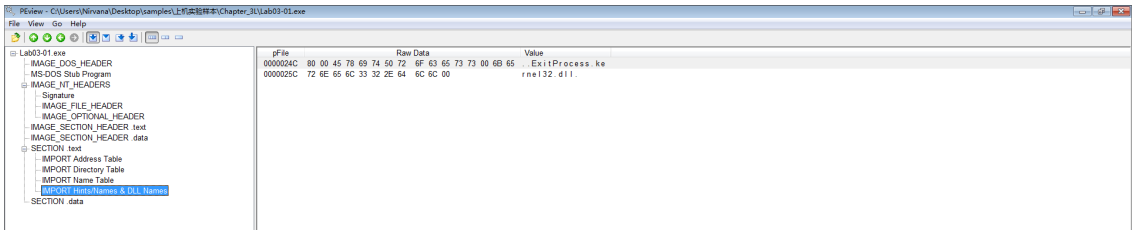


2. 使用PEview工具，得到Import信息如下：



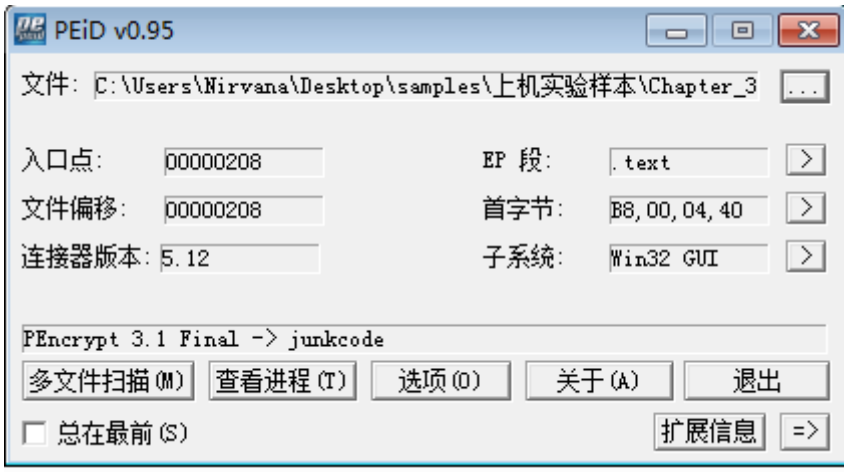






可以发现这个应用程序只导入了kernel32.dll，这个是不正常的，数量太少，由此猜测本程序存在有加壳，并且strings工具的检测结果也可以从侧面验证存在有壳。

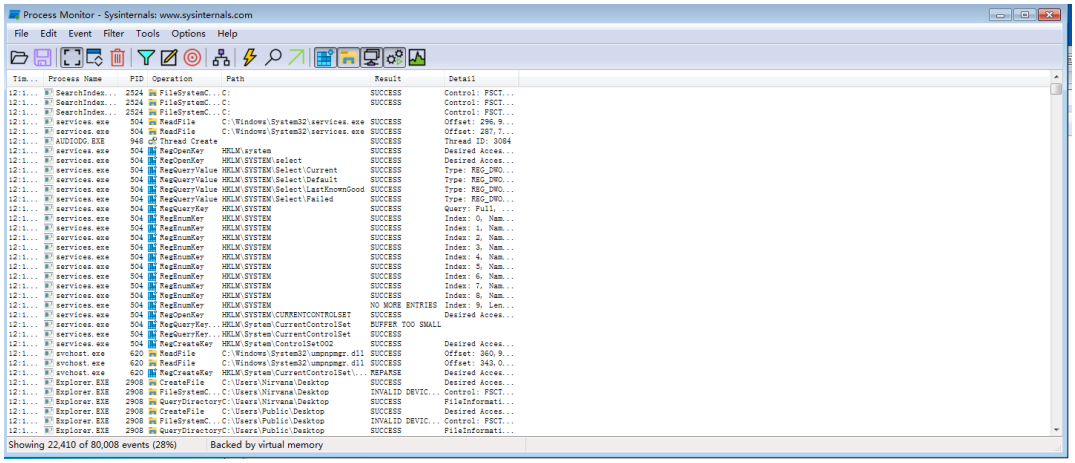
3. 使用PEiD工具验证是否有加壳



可以发现检测出来了存在有加壳，猜想正确

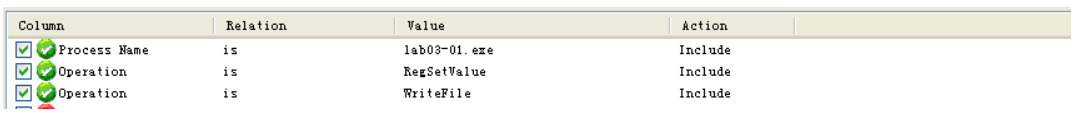
4. 进行动态检测

    1. 使用Process Monitor工具查看初始状态的进程监视状态如下：

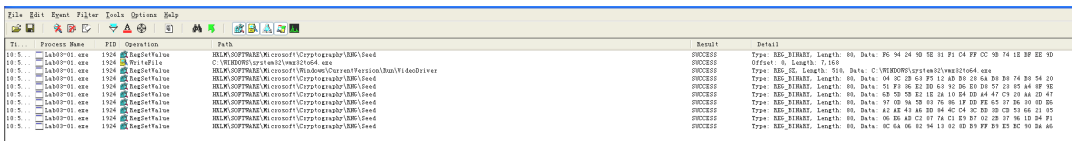


将当前状态进行清空，并运行lab03-01.exe

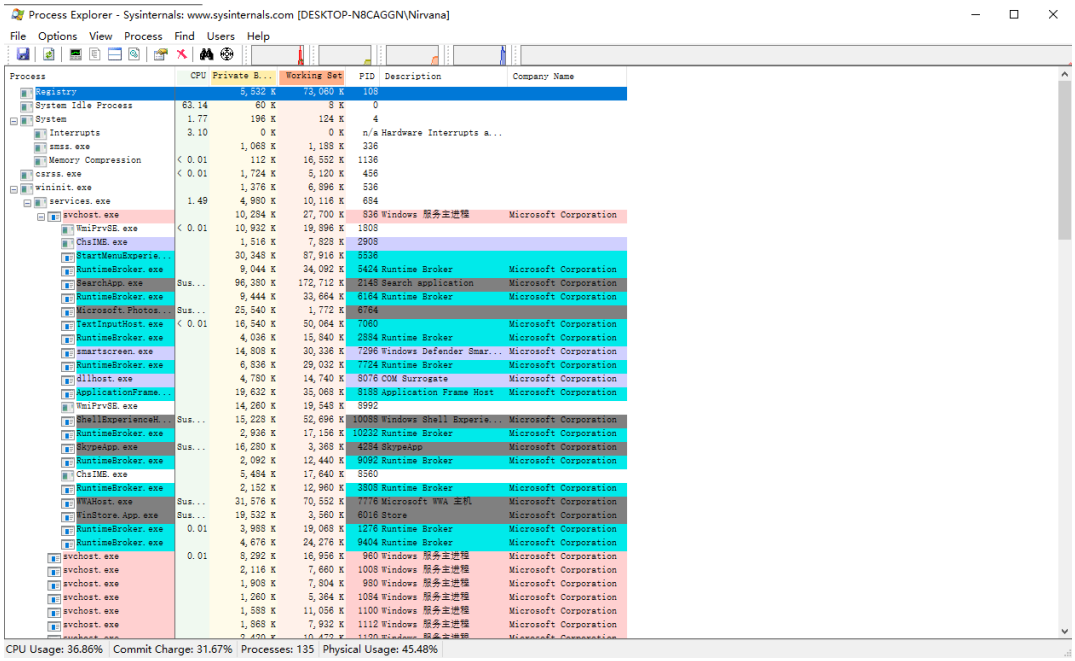
设置过滤条件为：



可以查看到当前过滤条件下得到的结果为：

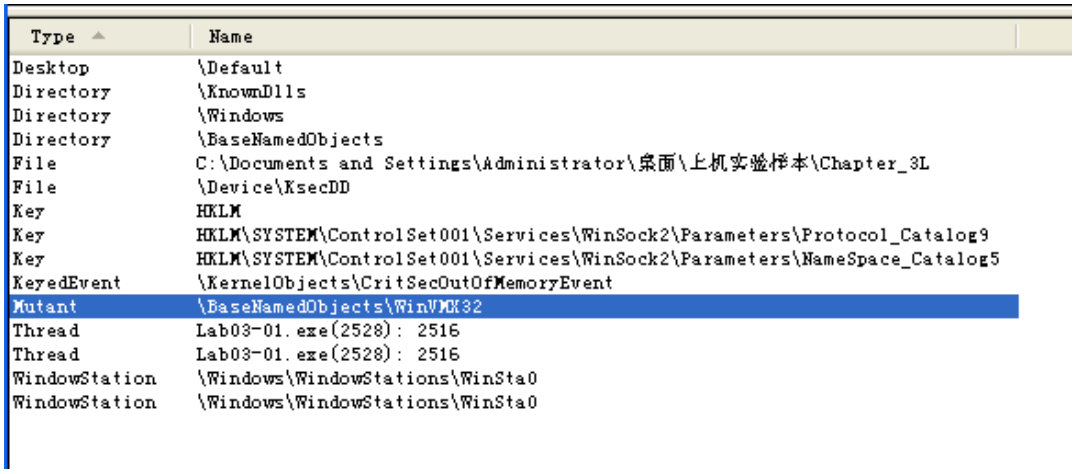


2. 使用Process Explorer工具查看初始状态的进程检查



运行lab03-01.exe

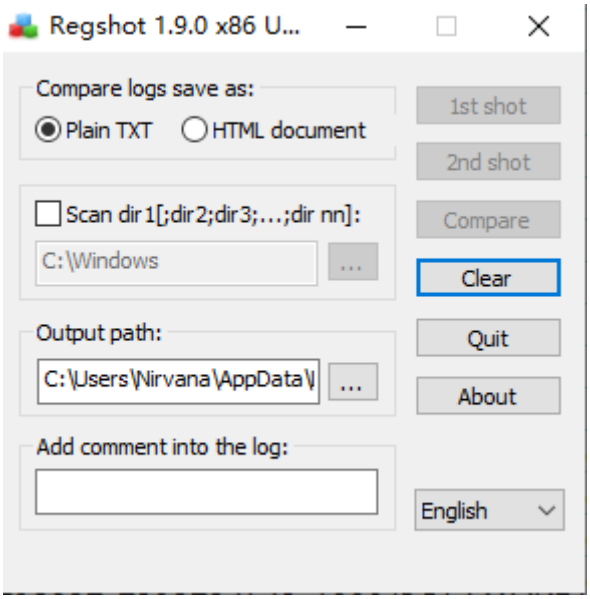
在Process Explorer的Handles视图中可以看到如下结果：



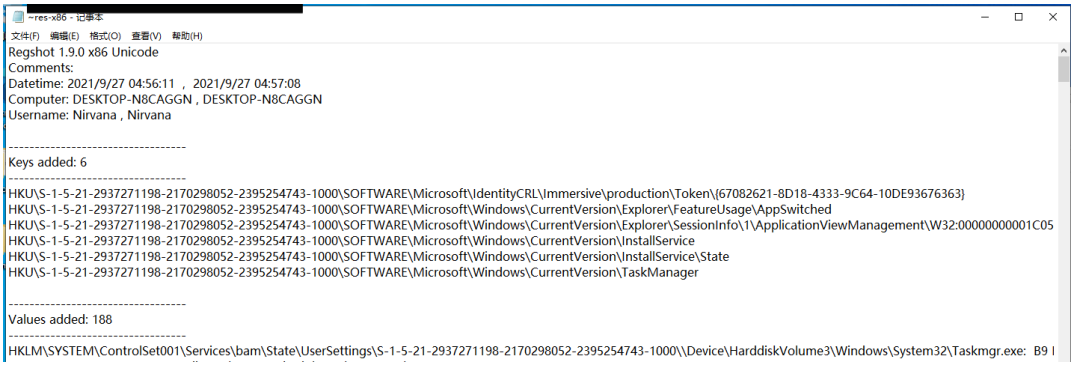
Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\Windows
Directory	\BaseNamedObjects
File	C:\Documents and Settings\Administrator\桌面\上机实验样本\Chapter_3L
File	\Device\KsecDD
Key	HKLM
Key	HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\Protocol_Catalog9
Key	HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\NameSpace_Catalog5
KeyedEvent	\KernelObjects\CritSecOutOfMemoryEvent
Mutant	\BaseNamedObjects\WinVMX32
Thread	Lab03-01.exe(2528): 2516
Thread	Lab03-01.exe(2528): 2516
WindowStation	\Windows\WindowStations\WinSta0
WindowStation	\Windows\WindowStations\WinSta0

可以发现这个进程创建了一个名为WinVMX32的互斥量

3. 使用RegShot工具，查看程序运行前后对注册表进行了什么样的操作



得到部分反馈结果为：

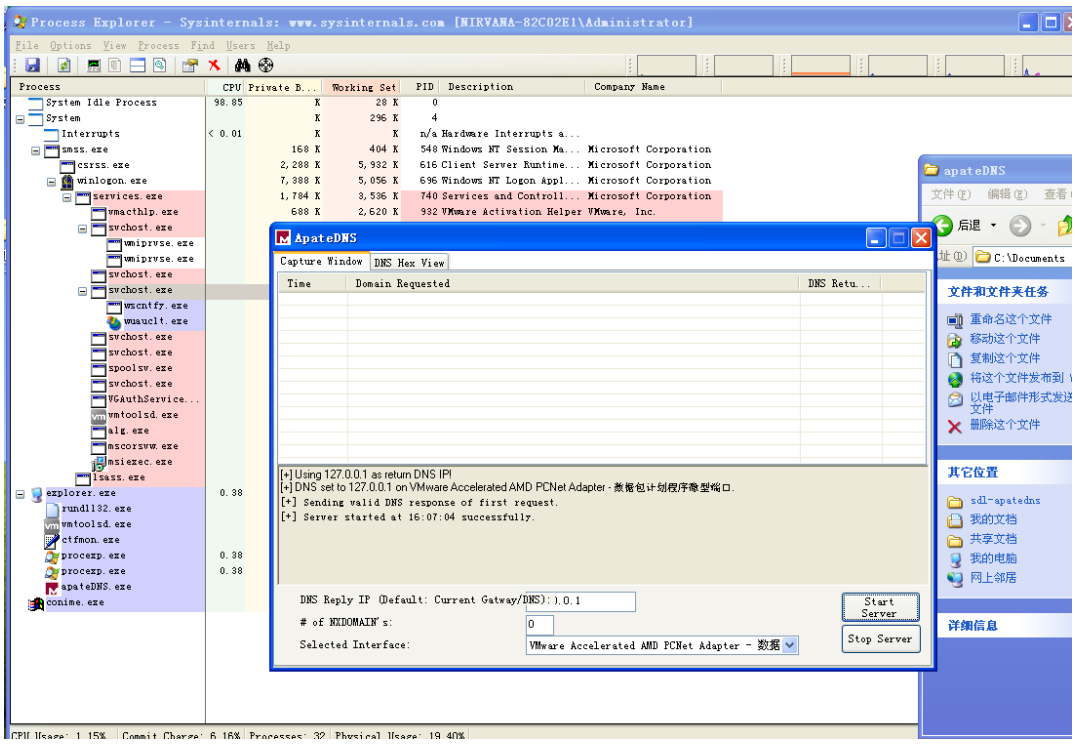


可以看见这个程序修改了注册表中的很多项目。其中有一个条目是`HKU\S-1-5-21-2937271198-2170298052-2395254743-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\InstallService`，还有之后的一个`HKU\S-1-5-21-2937271198-2170298052-2395254743-1000\SOFTWARE\Microsoft\Windows\CurrentVersion\InstallService\State`，可以看出这个应用安装了他所需要使用的服务。

但是在其中有一反馈的信息是：`\Software\Classes\Local Settings\MuiCache\a\AAF68885\@%SystemRoot%\System32\wersvc.dll,-100: "Windows Error Reporting Service"`，由此可以认为应当是服务未能正常启动，导致程序使用失败，才会有之前的进程仅运行了一小段时间就结束。

4. 获取网络行为

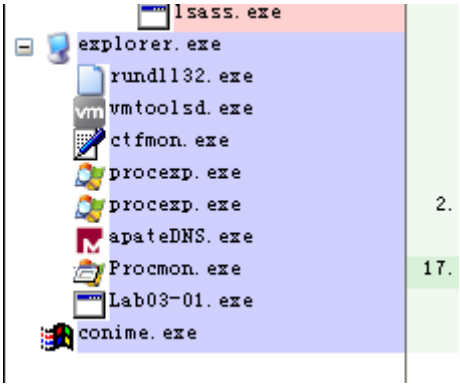
   首先启动process explorer和ApateDNS



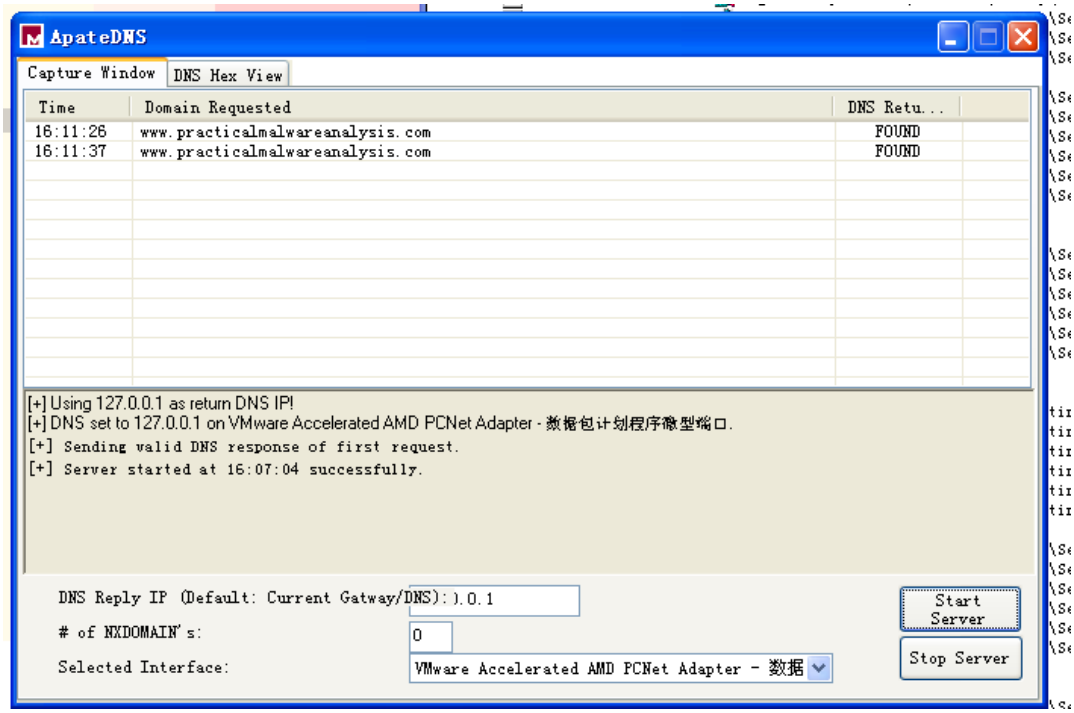
再启动procmon，清空当前状态，重新打开监视

待准备工作就绪以后，双击Lab03-01.exe，运行程序。

在process explorer中发现Lab03-01.exe这个进程



并且在ApateDNS中可以发现存在有网络访问的行为，访问的网址为`www.practicalmalwareanalysis.com`



Time	Domain Requested	DNS Retu...
16:11:26	www.practicalmalwareanalysis.com	FOUND
16:11:37	www.practicalmalwareanalysis.com	FOUND

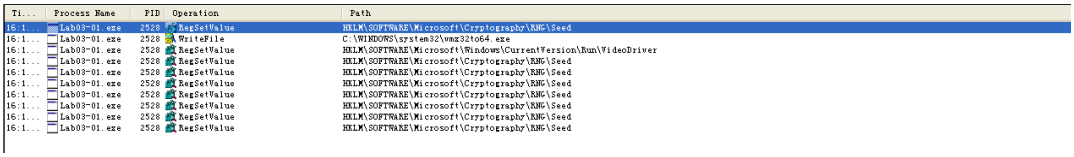
```
[+] Using 127.0.0.1 as return DNS IP!
[+] DNS set to 127.0.0.1 on VMware Accelerated AMD PCNet Adapter - 数据包计划程序微型端口.
[+] Sending valid DNS response of first request.
[+] Server started at 16:07:04 successfully.
```

DNS Reply IP (Default: Current Gatway/DNS):).0.1

# of NXDOMAIN's: 0

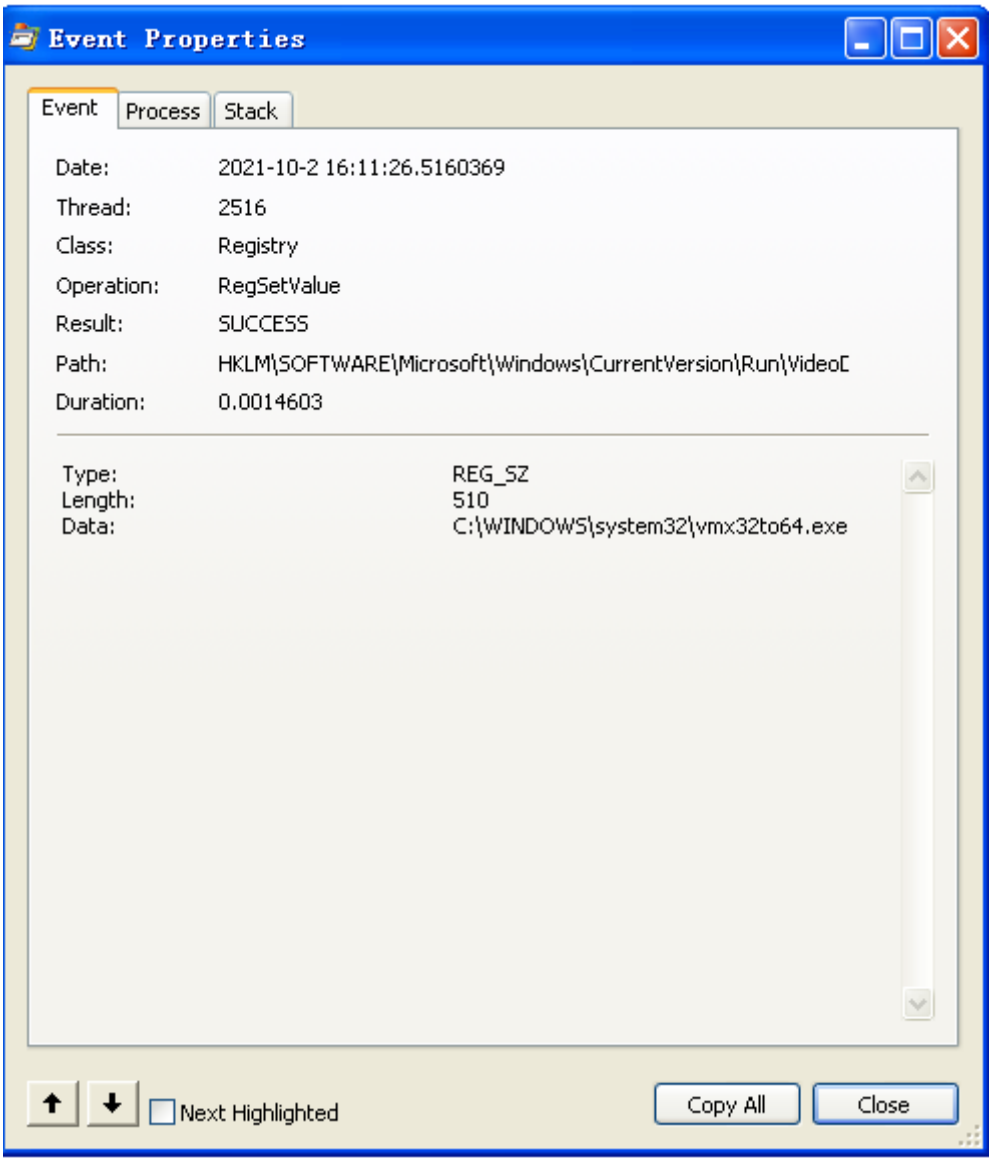
Selected Interface: VMware Accelerated AMD PCNet Adapter - 数据

在procmon中设置过滤条件，得到如下图的情况

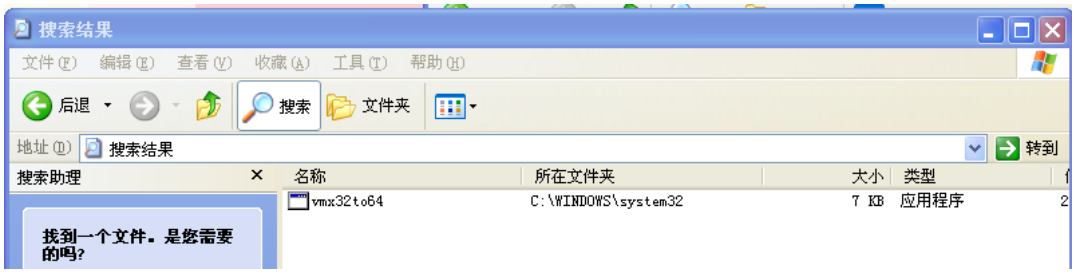


Ti...	Process Name	PID	Operation	Path
16:1...	Lab03-01.exe	2528	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
16:1...	Lab03-01.exe	2528	WriteFile	C:\WINDOWS\system32\vmx32to64.exe
16:1...	Lab03-01.exe	2528	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver
16:1...	Lab03-01.exe	2528	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
16:1...	Lab03-01.exe	2528	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
16:1...	Lab03-01.exe	2528	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
16:1...	Lab03-01.exe	2528	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
16:1...	Lab03-01.exe	2528	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
16:1...	Lab03-01.exe	2528	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed
16:1...	Lab03-01.exe	2528	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed

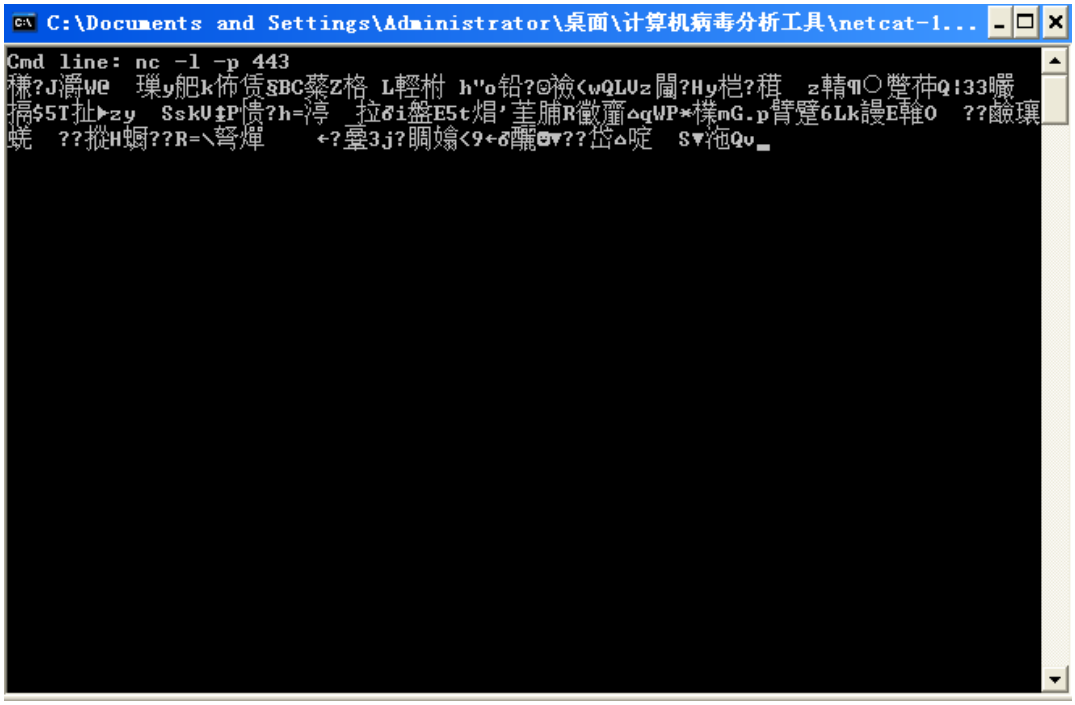
可以看到样本有对注册表的操作，也有创建文件、写文件的操作，虽然写文件的操作只有一条，但是却是在C:\WINDOWS\system32目录下创建了一个程序，这个是很关键的，同时经过对比lab03-01.exe和这个新创建的vmx32to64.exe可以发现这两个程序的Hash值是一样的，也就是说lab03-01.exe是在这个目录下创建了自己的一个副本；之后对注册表的操作虽然比较多，但是大部分是在设置种子，经过查阅资料发现，这个操作是典型的噪声。在注册表的操作中有一条是比较不一样的，也就是图中第三条操作，双击以后可以得到如下图所示信息：

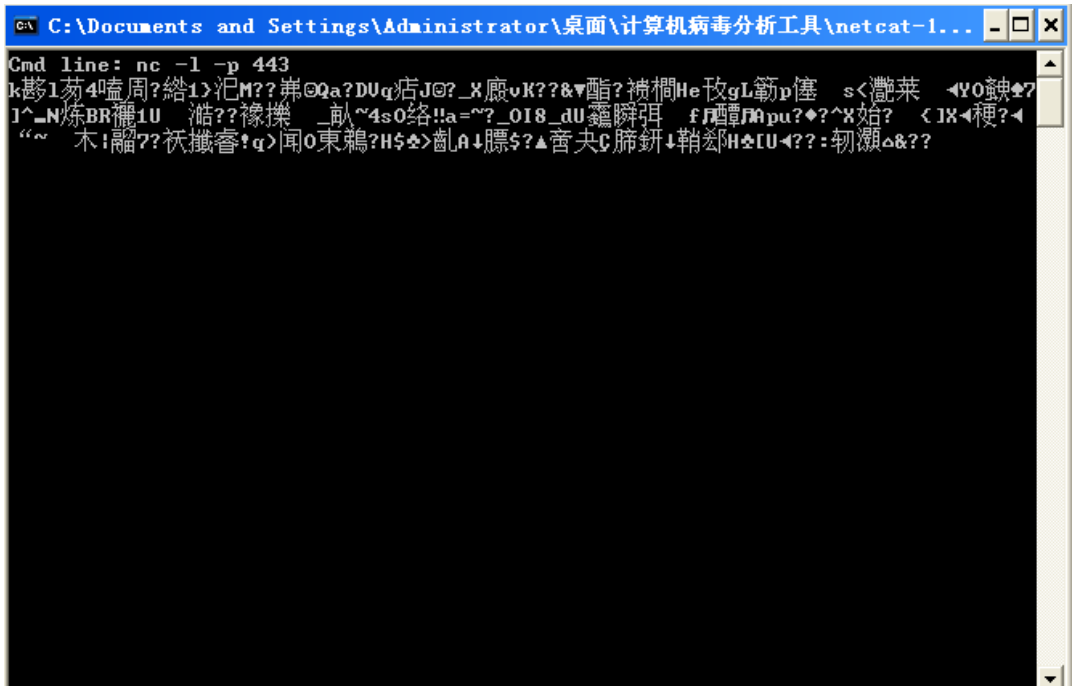


此时可以发现在C的system32目录下出现了一个名为vmx32to64.exe的程序



使用nc监视443端口（原本是想着这个是请求的一个url，应该去监视80端口，但是等待了很久并没有发现什么反馈），监视到下图信息：





可以发现每次检测到的数据都是不一样的，推测是和之前注册表中Seed的操作有关，不同的seed传递的应当是不同的数据。

问题回答

Q1

在实验过程中的1、2我们可以发现，strings工具检测出来的有用字符串是非常少的，并且PEview能够查看到的Import只有一个`ExitProcess`函数，这很明显是一个异常现象，也就是说这个文件应该是存在有加壳的。

但是在strings的结果中可以发现一些比较有用的信息，如：注册表、域名、vmx32to64.exe等

Q2

该样本创建了一个互斥量，名为：WinVMX32。并且在C:\Windows\System32的目录下创建了一个自己的副本：vmx32to64.exe，同时在注册表的Run下创建了一个自己的路径，使得副本能够自动执行。

Q3

该样本会对`www.practicalmalwareanalysis.com`这个域名进行解析和访问，并且会在443端口传输一些看上去是随机的数据，每次显示的数据都不一样。

lab 3-2

要求

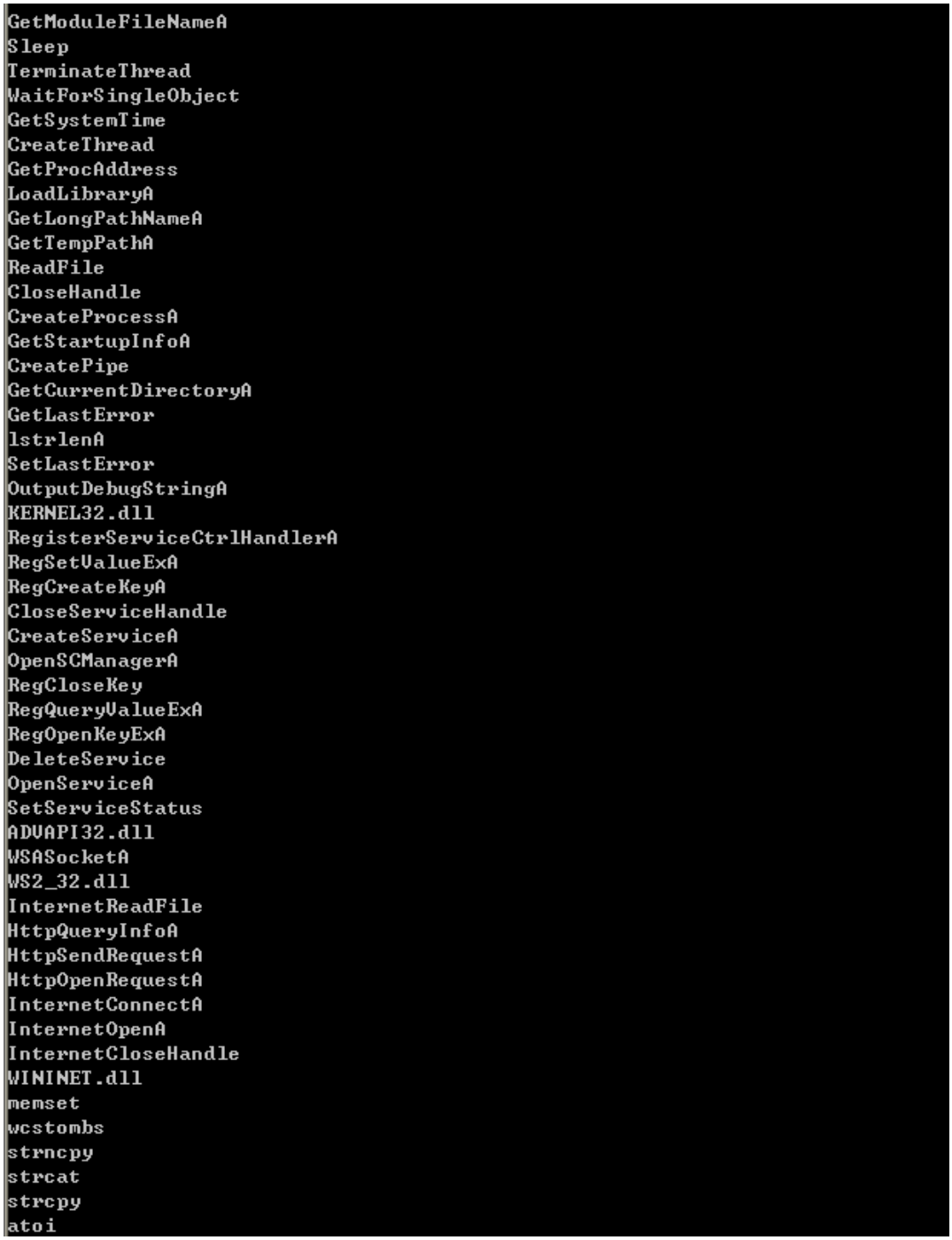
Analyze the malware found in the file *Lab03-02.dll* using basic dynamic analysis tools.

Questions

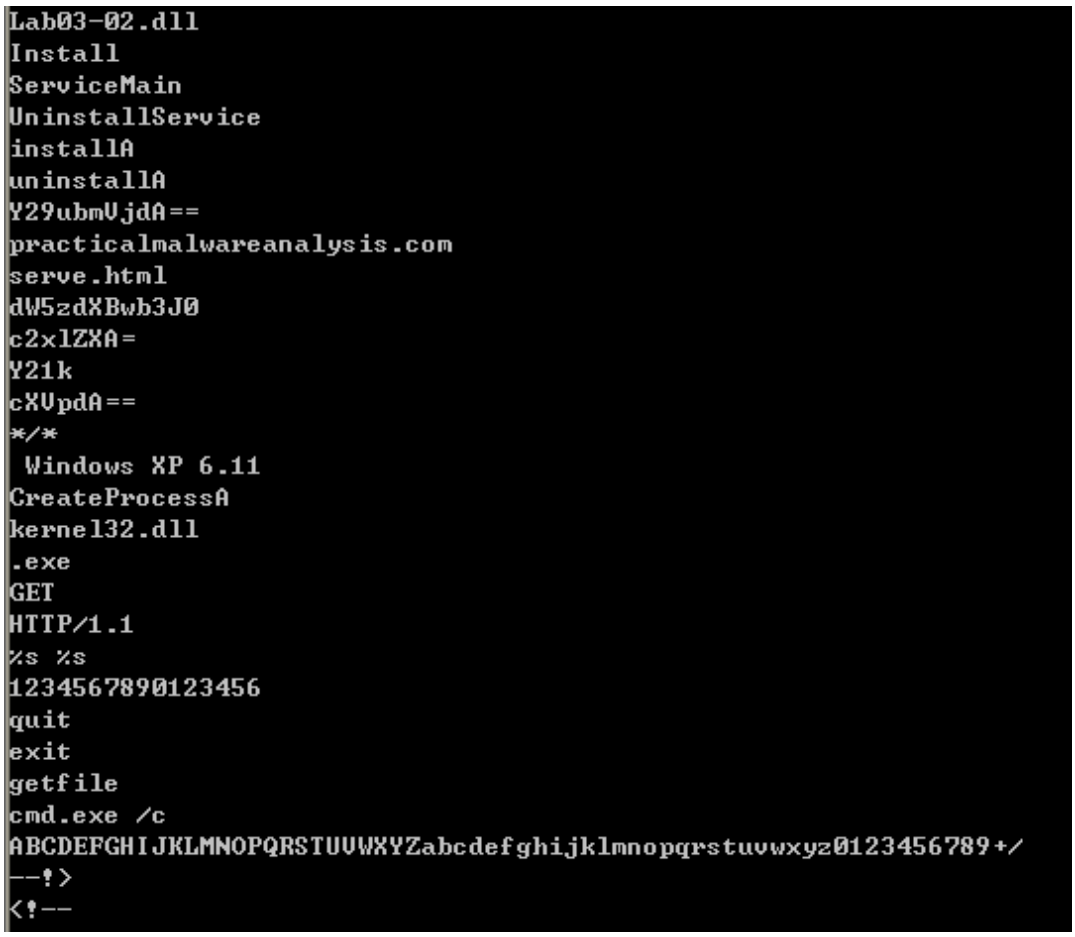
1. How can you get this malware to install itself?
2. How would you get this malware to run after installation?
3. How can you find the process under which this malware is running?
4. Which filters could you set in order to use procmon to glean information?
5. What are the malware's host-based indicators?
6. Are there any useful network-based signatures for this malware?

实验过程

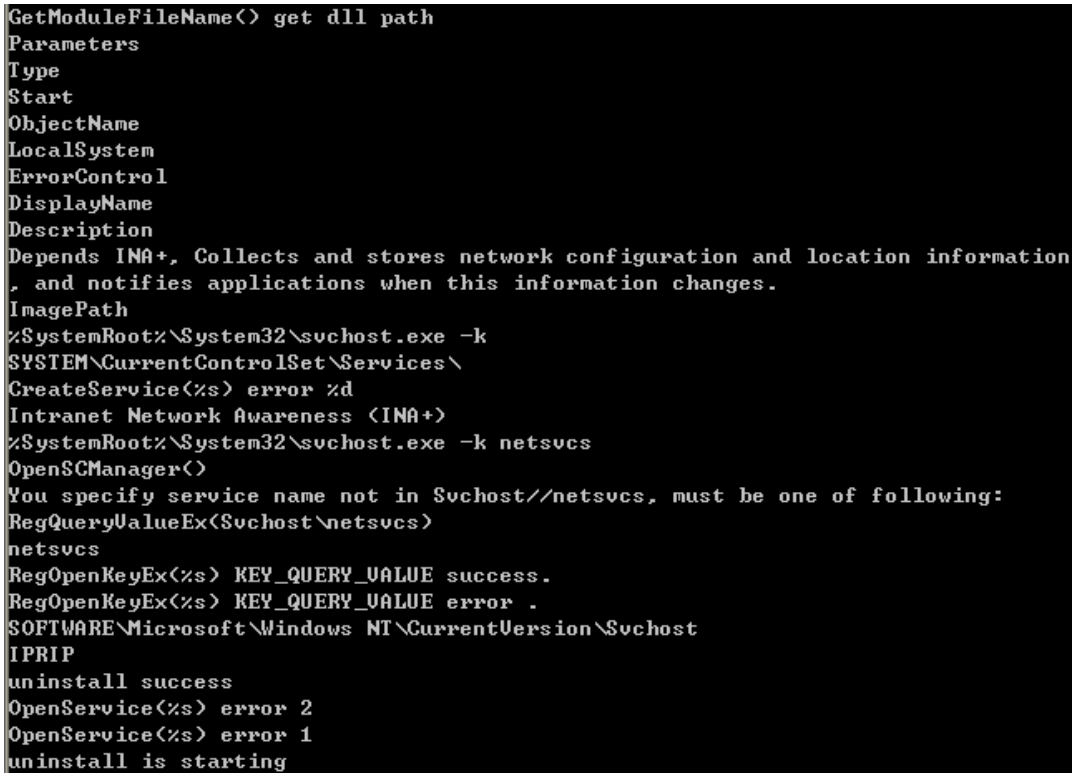
1. 先使用基础的静态分析
    1. 使用strings工具查看



在上面的字符串中可以看到了有获取系统时间、sleep、HTTP、strcpy等关键字样



第二幅图中出现了Lab03-02.dll，同时在下面还有Install、ServiceMain、practicalmalwareanalysis.com、CreateProcessA、Windows XP 6.11等字符串。



第三幅图中较多的字符串可以看出应该是提示的字符串。注意到其中有一个比较关键的字符串：`%SystemRoot%\System32\svchost.exe -k`，由此猜测这个程序可能是会运行一个名为svchost.exe的程序，并且给这个程序的参数是-k。

综合以上的字符串信息，猜测这个dll文件应该是需要安装、对注册表进行一些操作，安装之后会进行一些网络活动，并且会运行一个svchost.exe的程序，让其执行一些特殊的功能。

2. 使用PEview查看样本的导出表

pFile	Data	Description	Value
00004D3C	00005969	Function Name RVA	0001 Install
00004D40	00005978	Function Name RVA	0002 ServiceMain
00004D44	00005984	Function Name RVA	0003 UninstallService
00004D48	00005995	Function Name RVA	0004 installA
00004D4C	0000599E	Function Name RVA	0005 uninstallA

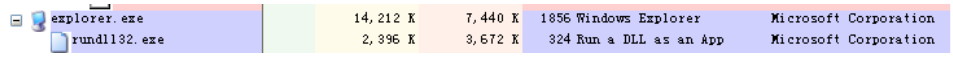
可以看到这个dll文件提供了Install和installA两个进行安装的函数，这个应该就是后面在使用rundll32.exe时需要使用的函数。

2. 使用基本的动态分析

    1. 执行安装，并使用RegShot工具监视注册表的变化

    使用rundll32.exe工具，执行命令`rundll32.exe Lab03-02.dll,installA`。

在process explorer中可以看见rundll32.exe此时正在运行



等到rundll程序执行结束后，查看运行前后注册表的变化：

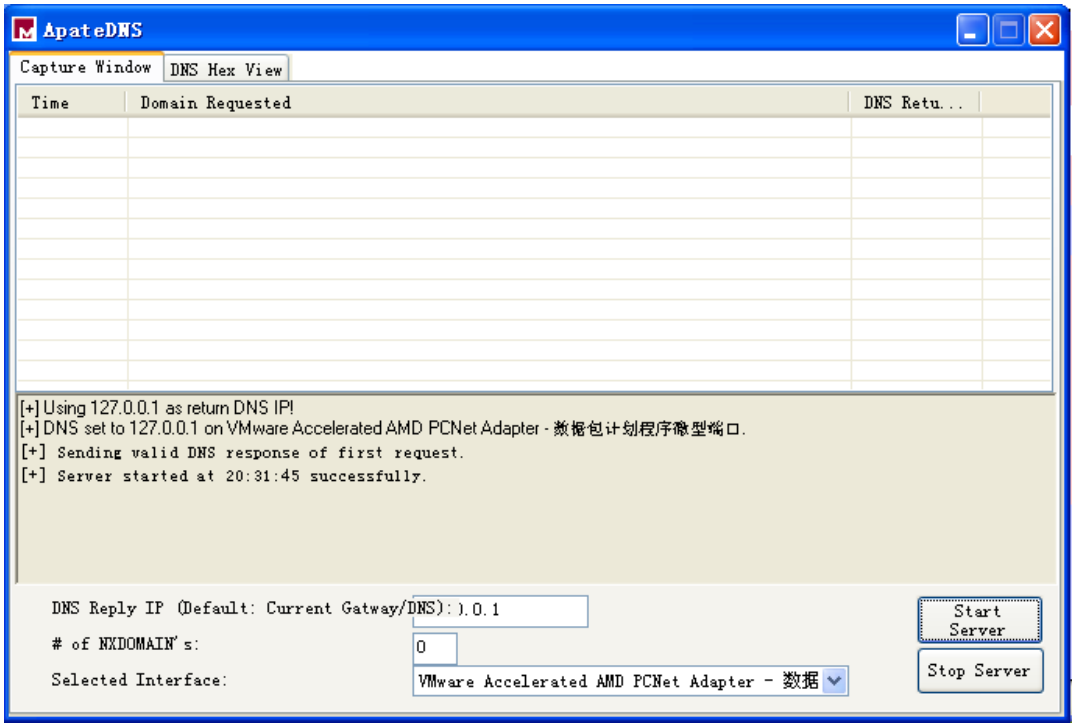
```
-----------------------------------
Keys added: 6
-----------------------------------
HKLM\SYSTEM\ControlSet001\Services\IPRIP
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security

-----------------------------------
Values added: 21
-----------------------------------
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Type: 0x00000020
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ImagePath:
"%SystemRoot%\System32\svchost.exe -k netsvcs"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DisplayName: "Intranet
Network Awareness (INA+)"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ObjectName: "LocalSystem"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Description: "Depends
INA+, Collects and stores network configuration and location
information, and notifies applications when this information
changes."
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DependOnService:  52 00 70
00 63 00 53 00 73 00 00 00 00 00
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters\ServiceDll:
"C:\Documents and Settings\Administrator\桌面\上机实验样本
\Chapter_3L\Lab03-02.dll"
```

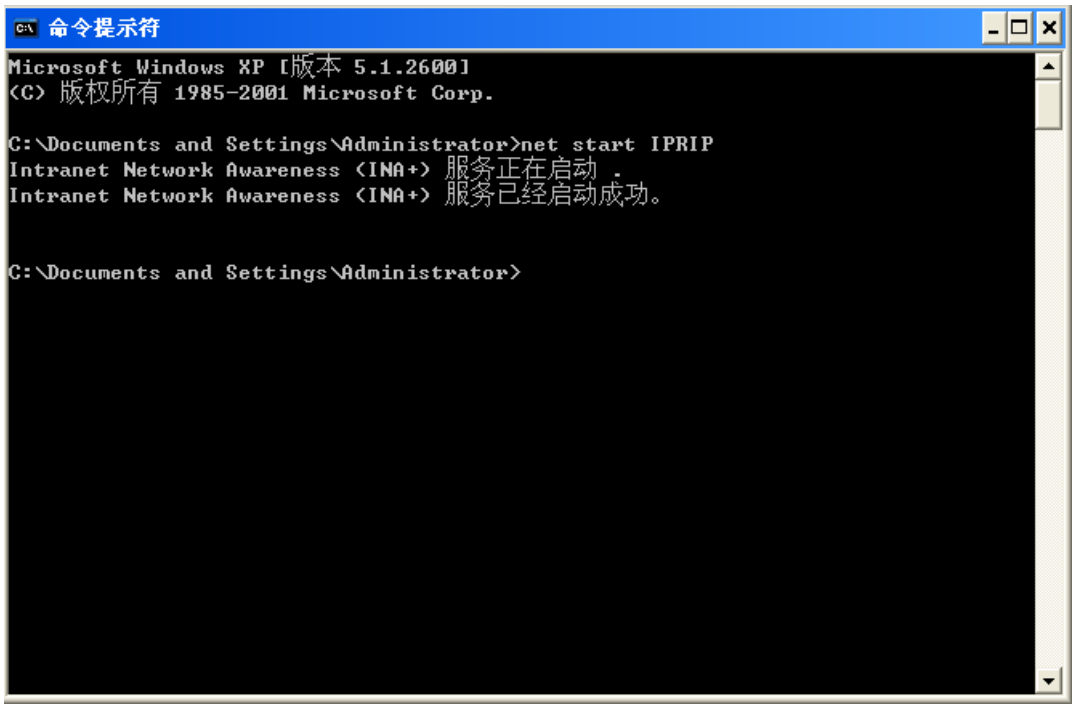
```
22 HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security\Security:  01 00
   14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00
   01 00 00 00 02 80 14 00 FF 01 0F 00 01 01 00 00 00 00 00 01 00 00
   00 00 02 00 60 00 04 00 00 00 00 00 14 00 FD 01 02 00 01 01 00 00
   00 00 00 05 12 00 00 00 00 00 18 00 FF 01 0F 00 01 02 00 00 00 00
   00 05 20 00 00 00 20 02 00 00 00 00 14 00 8D 01 02 00 01 01 00 00
   00 00 00 05 0B 00 00 00 00 00 18 00 FD 01 02 00 01 02 00 00 00 00
   00 05 20 00 00 00 23 02 00 00 01 01 00 00 00 00 00 05 12 00 00 00
   01 01 00 00 00 00 00 05 12 00 00 00
23 HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Type: 0x00000020
24 HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Start: 0x00000002
25 HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ErrorControl:
   0x00000001
26 HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ImagePath:
   "%SystemRoot%\System32\svchost.exe -k netsvcs"
27 HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\DisplayName: "Intranet
   Network Awareness (INA+)"
28 HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ObjectName:
   "LocalSystem"
29 HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Description: "Depends
   INA+, Collects and stores network configuration and location
   information, and notifies applications when this information
   changes."
30 HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\DependOnService:  52
   00 70 00 63 00 53 00 73 00 00 00 00 00
31 HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters\ServiceDll:
   "C:\Documents and Settings\Administrator\桌面\上机实验样本
   \Chapter_3L\Lab03-02.dll"
32 HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security\Security:  01
   00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 02 00 1C
   00 01 00 00 00 02 80 14 00 FF 01 0F 00 01 01 00 00 00 00 00 01 00
   00 00 00 02 00 60 00 04 00 00 00 00 00 14 00 FD 01 02 00 01 01 00
   00 00 00 00 05 12 00 00 00 00 00 18 00 FF 01 0F 00 01 02 00 00 00
   00 00 05 20 00 00 00 20 02 00 00 00 00 14 00 8D 01 02 00 01 01 00
   00 00 00 00 05 0B 00 00 00 00 00 18 00 FD 01 02 00 01 02 00 00 00
   00 00 05 20 00 00 00 23 02 00 00 01 01 00 00 00 00 00 05 12 00 00
   00 01 01 00 00 00 00 00 05 12 00 00 00
33 HKU\S-1-5-21-776561741-1123561945-725345543-
   500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\
   {75048700-EF1F-11D0-9888-
   006097DEACF9}\Count\HRZR_EHACVQY:%pfvqy2%\附件\命令提示符.yax:  01 00
   00 00 06 00 00 00 F0 FD FC E2 E8 B5 D7 01
```

从前面的对注册表信息的操作可以看出，样本将自身安装成了一个IPRIP的服务。同时有一个ImagePath，可以看见他设置成了svchost.exe，这也就意味着这个dll会被一个叫svchost.exe的程序调用、执行。

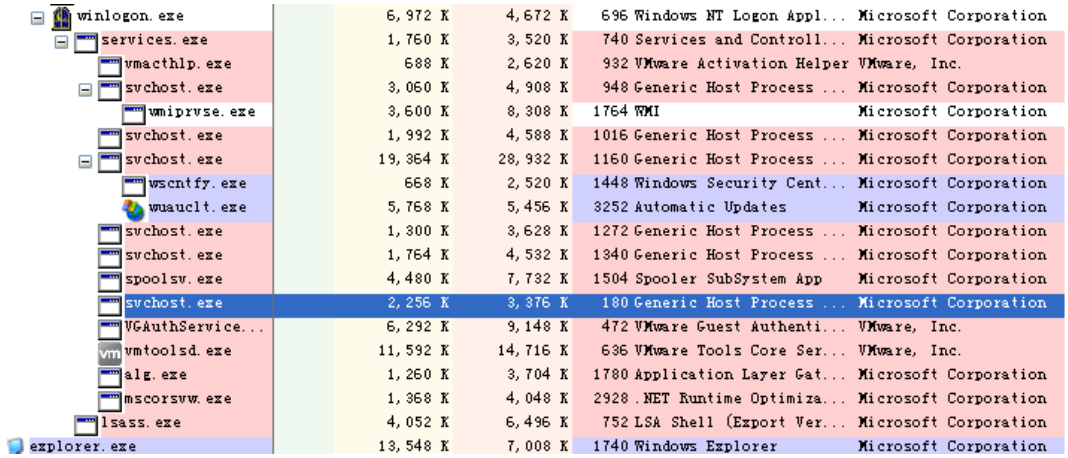
2. 启动服务并监控网络行为



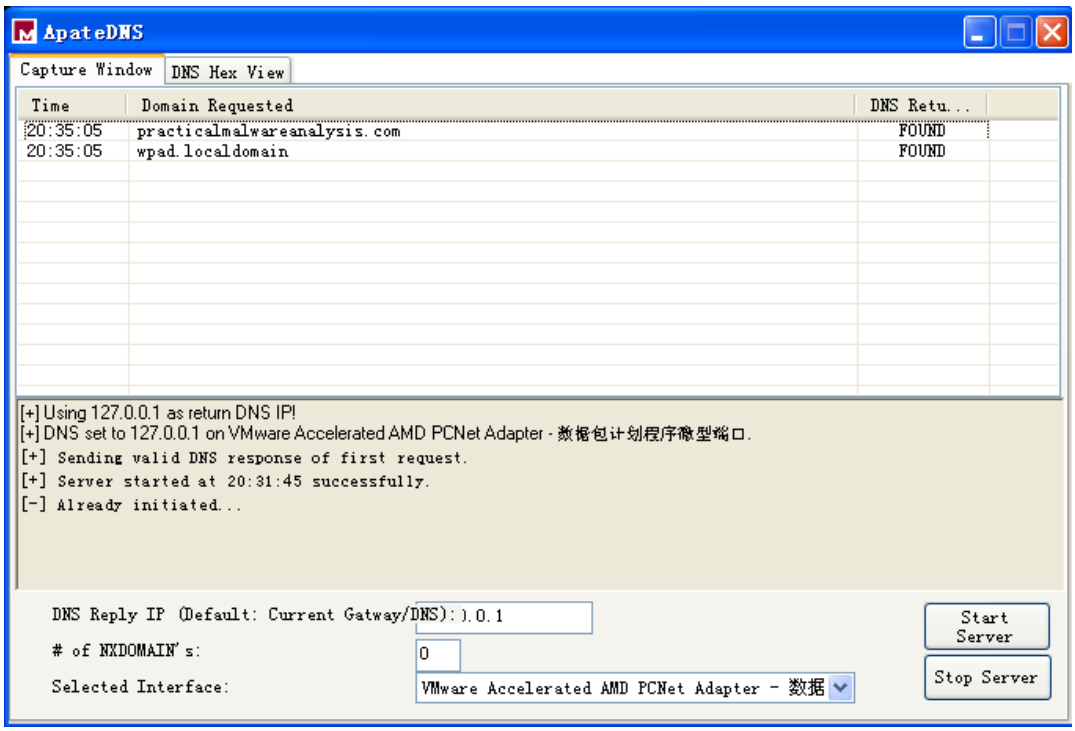
启动服务



根据刚刚在注册表中对信息的分析，可以看见在process explorer中有一个名为svchost.exe的进程在services.exe下运行



在大概过了一分钟左右，ApateDNS中捕获到相关网络行为



同时在nc中可以发现svchost.exe在80端口发送了一个GET请求

```
C:\Documents and Settings\Administrator\桌面\计算机病毒分析工具\netcat-1.11\netcat-1.11>nc -l -p 80
GET /serve.html HTTP/1.1
Accept: */*
User-Agent: nirvana-82c02e1 Windows XP 6.11
Host: practicalmalwareanalysis.com
```

我们发现这个请求的对象是serve.html，并且在User-Agent看见了自己的xp系统上用的用户名。

问题回答

Q1

通过strings工具的分析，可以回到这个dll应该是使用installA这个函数进行服务的安装，所以这里利用了rundll32.exe工具进行安装，具体的执行指令为：`rundll32.exe Lab03-02.dll,installA`

Q2

通过之前对注册表的分析可以知道，这个程序是将自己注册成了IPRIP服务，而对于服务的启动，只需要运行指令：`net start IPRIP`即可

Q3

在process explorer中可以确定当前有哪个进程正在运行服务。从之前的分析可以得出这个dll文件的执行应该是依附于svchost.exe上的，所以只需要在process explorer中找到这个服务并查看即可。

Q4

在procmon里有很多的过滤方式，如果要定位某个进程，可以使用Filter中的process name方式进行过滤，或者是使用process explorer中发现的PID在procmon中过滤

Q5

这个样本会注册一个IPRIP服务，并且会将自己写入在注册表中。

Q6

通过之前在strings中的分析，可以发现有一个`practicalmalwareanalyseis.com`域名，由此这个样本应该是通过此域名，并通过80端口连接到本机，使用的请求方式是GET，请求的资源是`serve.html`。同时在前面的分析过程中可以看到有`HttpSendRequestA`等函数，由此应该是使用的HTTP协议。

lab 3-3

要求

Execute the malware found in the file *Lab03-03.exe* while monitoring it using basic dynamic analysis tools in a safe environment.

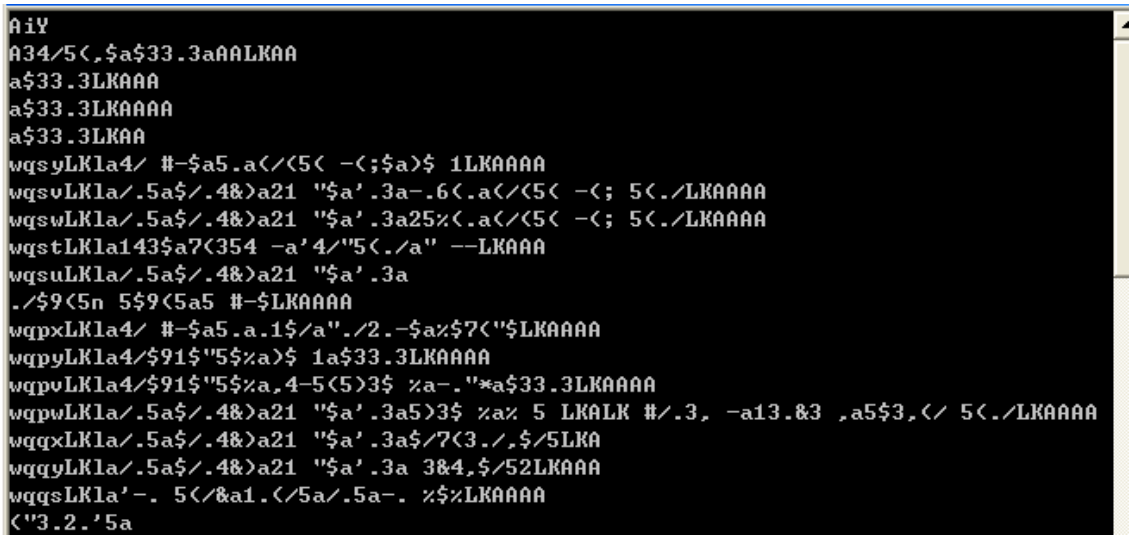
Questions

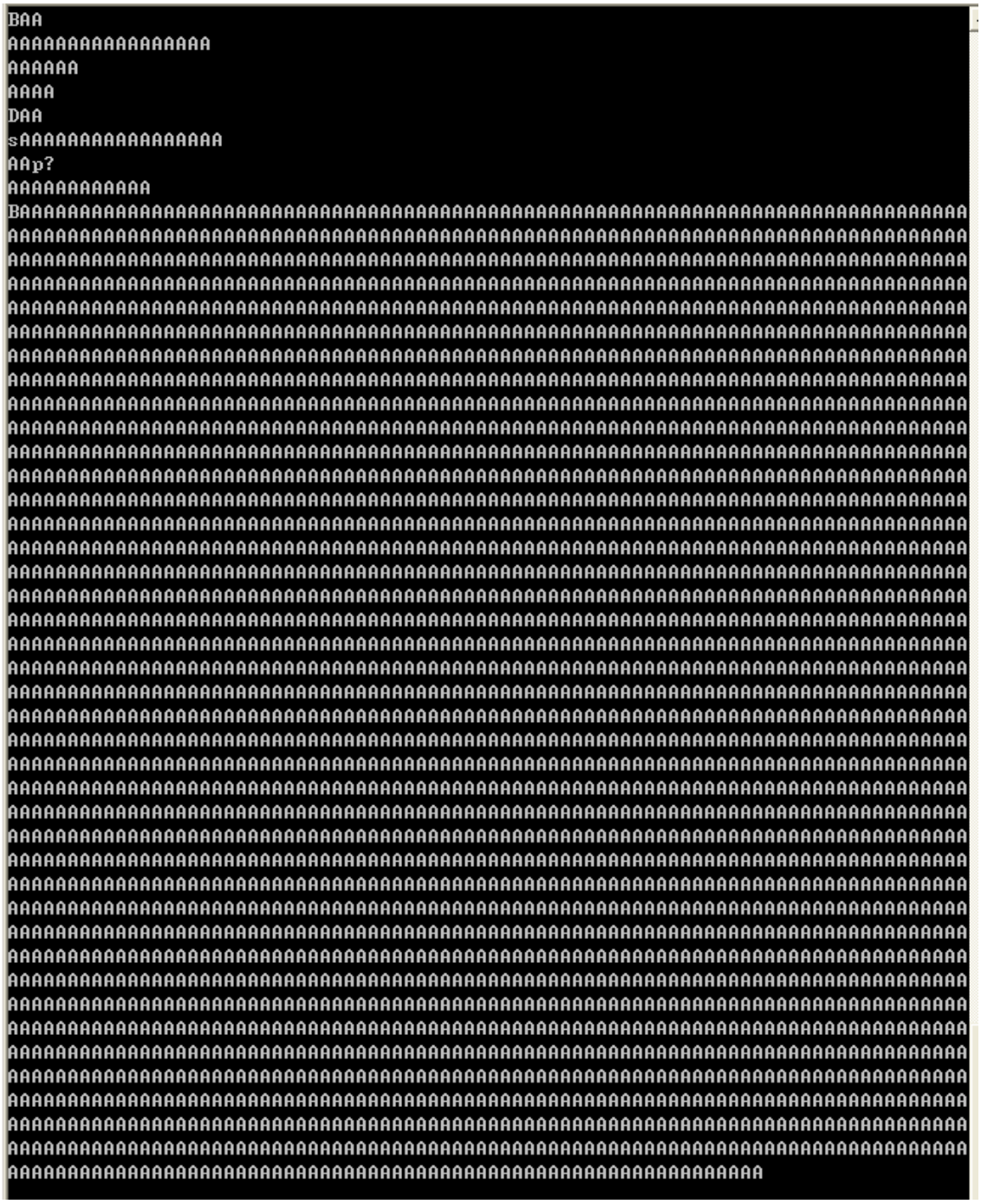
1. What do you notice when monitoring this malware with Process Explorer?
2. Can you identify any live memory modifications?
3. What are the malware's host-based indicators?
4. What is the purpose of this program?

实验过程

1. 首先使用基础的静态分析查看一下当前文件

   使用strings工具



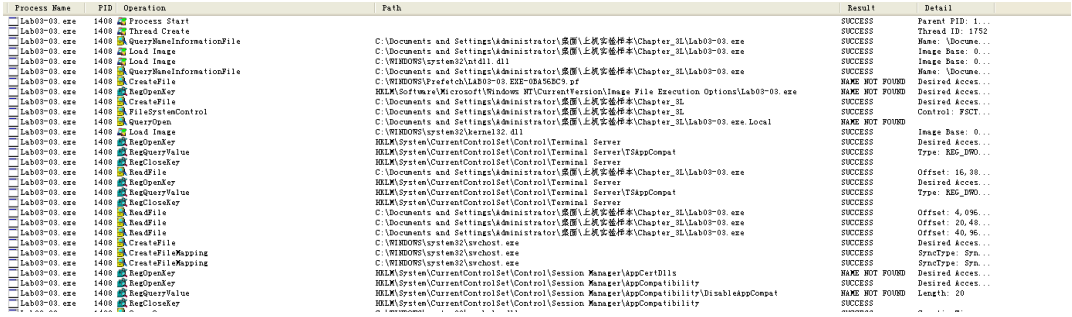


可以看到得到了非常多的无用字符串，由此可以认为这个程序应当是进行过混淆的，只是通过静态是完全无法分析的。

2. 对样本进行基础的动态分析

    1. 首先启动procmon、process explorer，双击执行样本

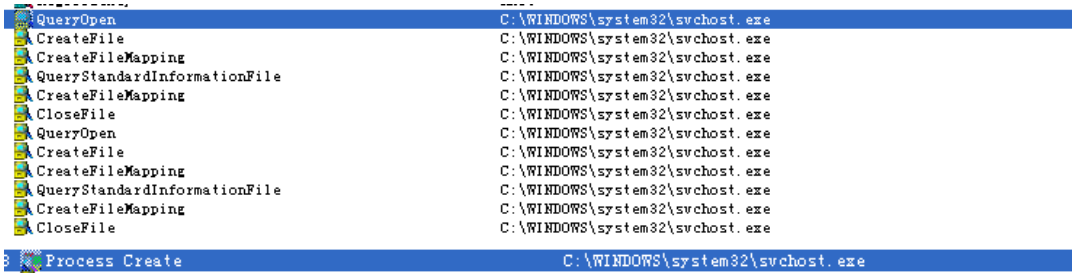
        在procmon中过滤以后呈现结果：



Process Name	PID	Operation	Path	Result	Detail
Lab03-03.exe	1408	Process Start		SUCCESS	Parent PID: 1...
Lab03-03.exe	1408	Thread Create		SUCCESS	Thread ID: 1752
Lab03-03.exe	1408	QueryNameInformationFile	C:\Documents and Settings\Administrator\桌面\上机实验样本\Chapter_3L\Lab03-03.exe	SUCCESS	Name: \Docume...
Lab03-03.exe	1408	Load Image	C:\Documents and Settings\Administrator\桌面\上机实验样本\Chapter_3L\Lab03-03.exe	SUCCESS	Image Base: 0...
Lab03-03.exe	1408	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0...
Lab03-03.exe	1408	QueryNameInformationFile	C:\Documents and Settings\Administrator\桌面\上机实验样本\Chapter_3L\Lab03-03.exe	SUCCESS	Name: \Docume...
Lab03-03.exe	1408	CreateFile	C:\WINDOWS\Prefetch\LAB03-03.EXE-0BA56BC9.pf	NAME NOT FOUND	Desired Acces...
Lab03-03.exe	1408	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Lab03-03.exe	NAME NOT FOUND	Desired Acces...
Lab03-03.exe	1408	CreateFile	C:\Documents and Settings\Administrator\桌面\上机实验样本\Chapter_3L	SUCCESS	Desired Acces...
Lab03-03.exe	1408	FileSystemControl	C:\Documents and Settings\Administrator\桌面\上机实验样本\Chapter_3L	SUCCESS	Control: FSCT...
Lab03-03.exe	1408	QueryOpen	C:\Documents and Settings\Administrator\桌面\上机实验样本\Chapter_3L\Lab03-03.exe.Local	NAME NOT FOUND	
Lab03-03.exe	1408	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0...
Lab03-03.exe	1408	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Acces...
Lab03-03.exe	1408	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWO...
Lab03-03.exe	1408	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
Lab03-03.exe	1408	ReadFile	C:\Documents and Settings\Administrator\桌面\上机实验样本\Chapter_3L\Lab03-03.exe	SUCCESS	Offset: 16,38...
Lab03-03.exe	1408	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Acces...
Lab03-03.exe	1408	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWO...
Lab03-03.exe	1408	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
Lab03-03.exe	1408	ReadFile	C:\Documents and Settings\Administrator\桌面\上机实验样本\Chapter_3L\Lab03-03.exe	SUCCESS	Offset: 4,096...
Lab03-03.exe	1408	ReadFile	C:\Documents and Settings\Administrator\桌面\上机实验样本\Chapter_3L\Lab03-03.exe	SUCCESS	Offset: 20,48...
Lab03-03.exe	1408	ReadFile	C:\Documents and Settings\Administrator\桌面\上机实验样本\Chapter_3L\Lab03-03.exe	SUCCESS	Offset: 40,96...
Lab03-03.exe	1408	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Acces...
Lab03-03.exe	1408	CreateFileMapping	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: Syn...
Lab03-03.exe	1408	CreateFileMapping	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: Syn...
Lab03-03.exe	1408	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls	NAME NOT FOUND	Desired Acces...
Lab03-03.exe	1408	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility	SUCCESS	Desired Acces...
Lab03-03.exe	1408	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility\DisableAppCompat	NAME NOT FOUND	Length: 20
Lab03-03.exe	1408	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatibility	SUCCESS	

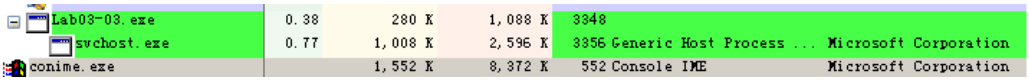
        通过查看procmon显示的结果，我们发现这个样本有一些需要关注的行为：创建线程，加载图像、创建文件等。

其中有一个比较关键的是：他创建了另一个应用程序：`svchost.exe`，并且将这个应用程序运行起来，相关截图如下：

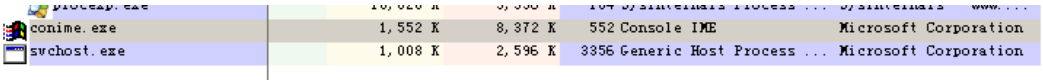


同时在process explorer中可以发现，lab03-03.exe会创建一个子进程svchost.exe，然后将自己关闭，只留下原本创建的子进程，相关截图如下：

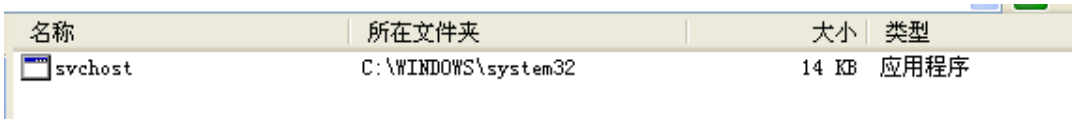
刚开始运行：



一段时间后：



2. 在磁盘上找到创建的svchost.exe这个程序的文件

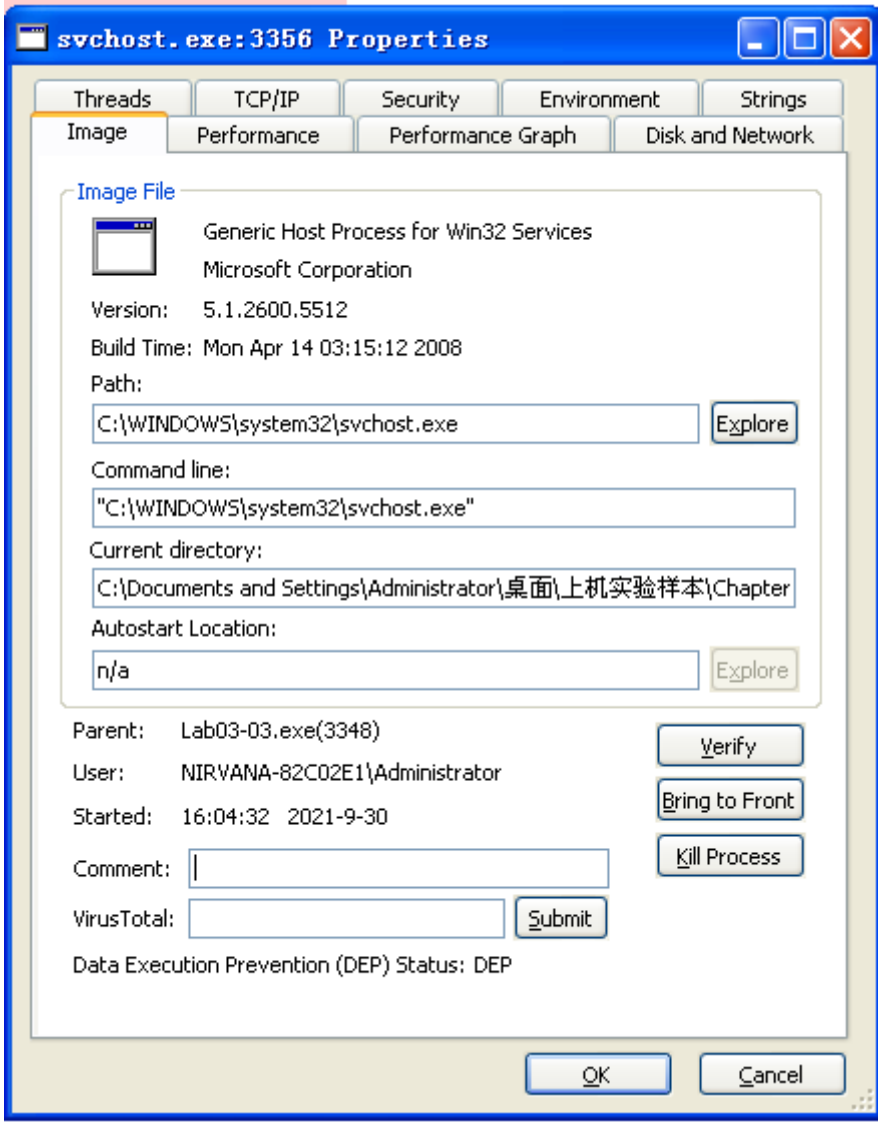


发现这个程序的源文件大小只有14KB

3. 查看内存中svchost.exe的情况

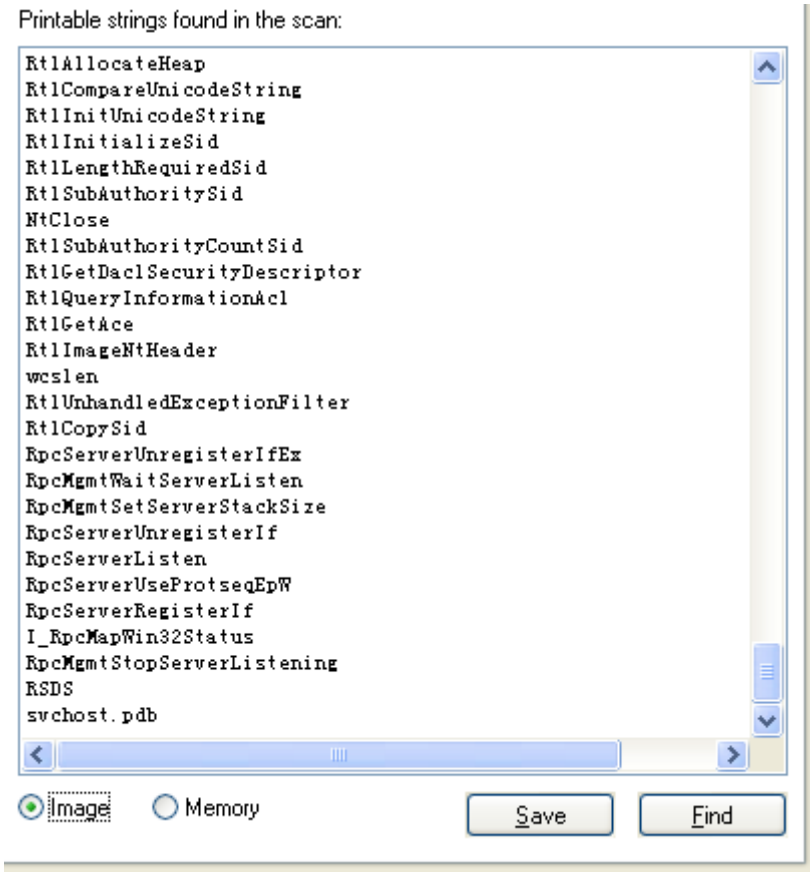
在precess explorer中可以看见这个程序真正占用的一些空间应该是远超过14kb的

右键-properties，可以看到如下信息：

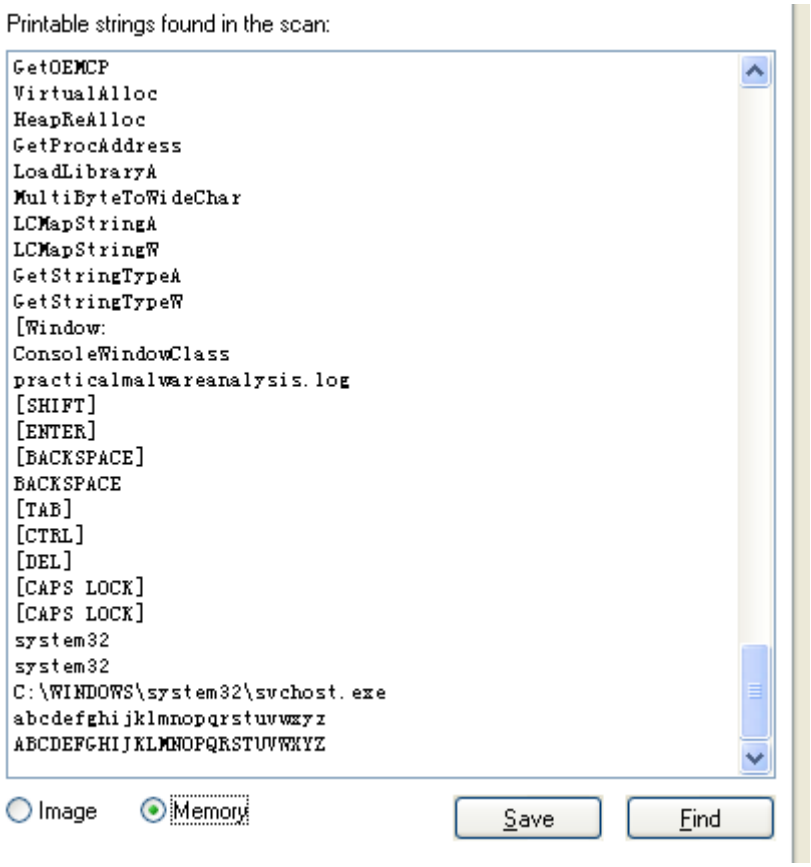


查看strings中在images和memory分别是什么样的

images中：

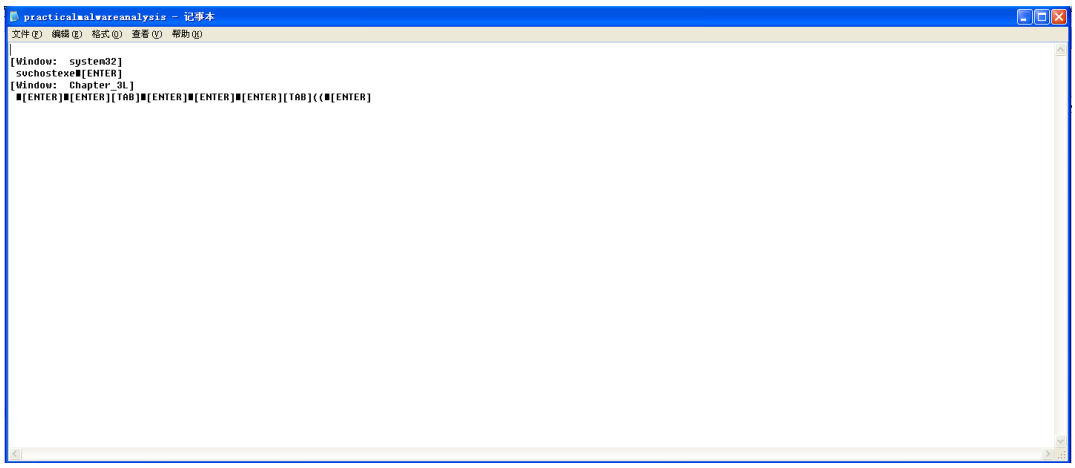


memory中：



可以发现这个程序在内存中和在磁盘上的差距还是很大的，并且在内存中有一个.log文件的字样，并且还有[SHIFT]、[ENTER]等字样，根据这些可以猜测到这个程序应该是会有一个日志记录，去抓取键盘操作。同时因为内存和磁盘中的strings区别很大，还可以推测出这个程序应该是做了进程替换。

之后在系统中按了几下回车键，并全局搜索practicalmalwareanalysis.log文件，最终找到这个日志文件就存放在和lab03-03.exe同目录下，打开以后可以看见记录了刚刚敲回车的记录。



问题回答

Q1

这个程序创建了一个子进程svchost.exe以后将自身清除，只留下了svchost.exe继续运行，达到了替换的目的。

Q2

通过process explorer中的磁盘和内存中string的对比，可以明显的发现内存中的string要比磁盘中的多不少，比如要记录的日志的名称`practicalmalwareanalysis.log`，以及一些[ENTER]、[TAB]等。

Q3

比较直观的、能够看见的是在windows\system32目录下创建了svchost.exe，并且在lab03-03.exe的同目录下创建了practicalmalwareanalysis.log文件。

Q4

执行进程替换，记录键盘输入的内容（但是不是针对所有的输入，只对类似于enter、tab等这类具有特殊功能的按键进行了记录）

lab 3-4

要求

Analyze the malware found in the file *Lab03-04.exe* using basic dynamic analysis tools. (This program is analyzed further in the Chapter 9 labs.)

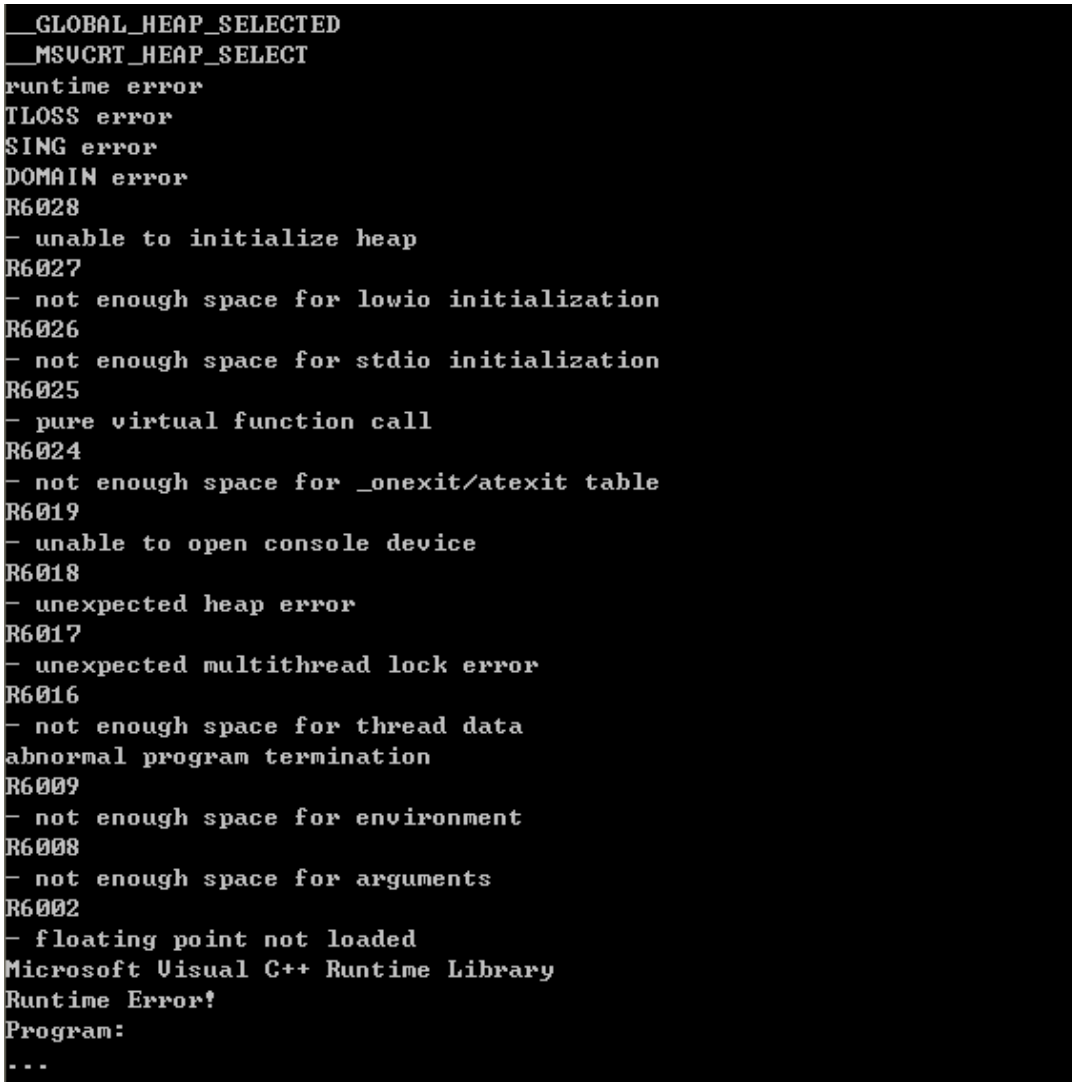
Questions

1. What happens when you run this file?
2. What is causing the roadblock in dynamic analysis?
3. Are there other ways to run this program?

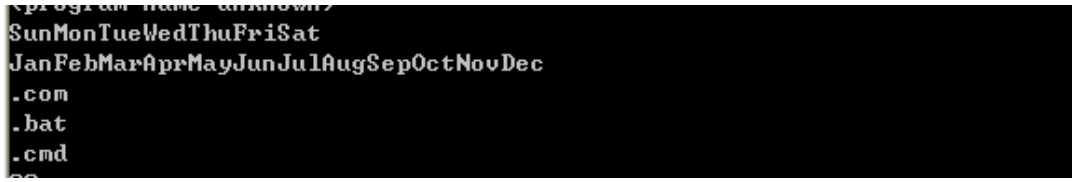
实验过程

1. 先对样本进行简单的静态分析

1. 使用strings工具查看字符串



上图中的字符串，可以看见都是一些提示信息， 猜测应当是这个病毒在执行时，如果遇见一些问题时会提示的信息



上图中的字符串可以发现有关于日期的提示，猜测在程序中会显示当前日期的行为；同时有.com/.bat/.cmd字样，推测此程序的运行环境应当是在cmd环境下运行的，或者是在运行了以后会启动一个命令行

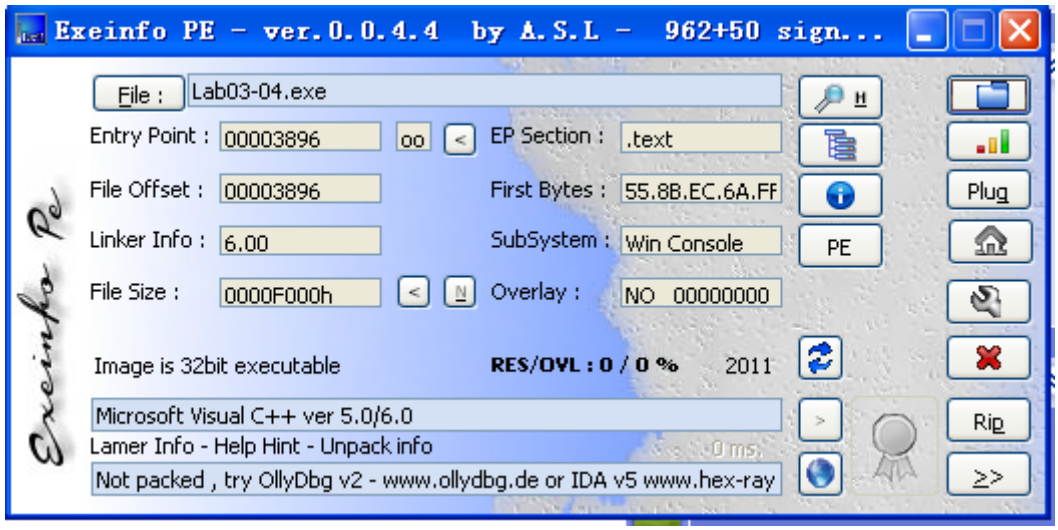
上图中的字符串则是当前程序使用的一些动态链接库或者是函数名，并且发现这上面的字符串是非常多的，推测此程序应当是没有进行加壳或混淆的。

```
 HTTP/1.0
GET
',',',
',',',
NOTHING
CMD
DOWNLOAD
UPLOAD
SLEEP
cmd.exe
 >> NUL
/c del
ups
http://www.practicalmalwareanalysis.com
 Manager Service
.exe
%SYSTEMROOT%\system32\
k:%s h:%s p:%s per:%s
-cc
-re
-in
```

上图中的字符串出现了有www.字样，由此可以认为这个应用程序应当是有网络行为的，并且访问的网址是`www.practiclamalwareanalysis.com`，同时发送的应当是GET请求。同时在最下面可以看到有疑似注册表的字样，猜测可能存在有修改注册表的行为。并且在最下面有`-cc`，`-re`，`-in`字样，联系之前推测运行环境应该是CMD，这里可能是在cmd环境下运行时的参数。

2. 查看是否存在加壳

   使用Exeinfo工具查看



   发现此程序确实是没有进行加壳的

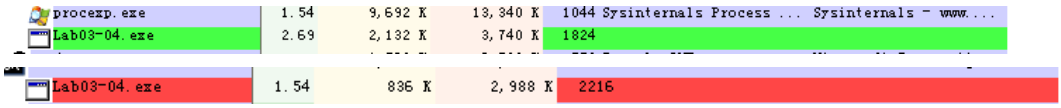
   使用PEiD工具查看

同样也是没有检测到壳的存在

由此验证了之前在strings中猜测次程序没有进行加壳的猜测

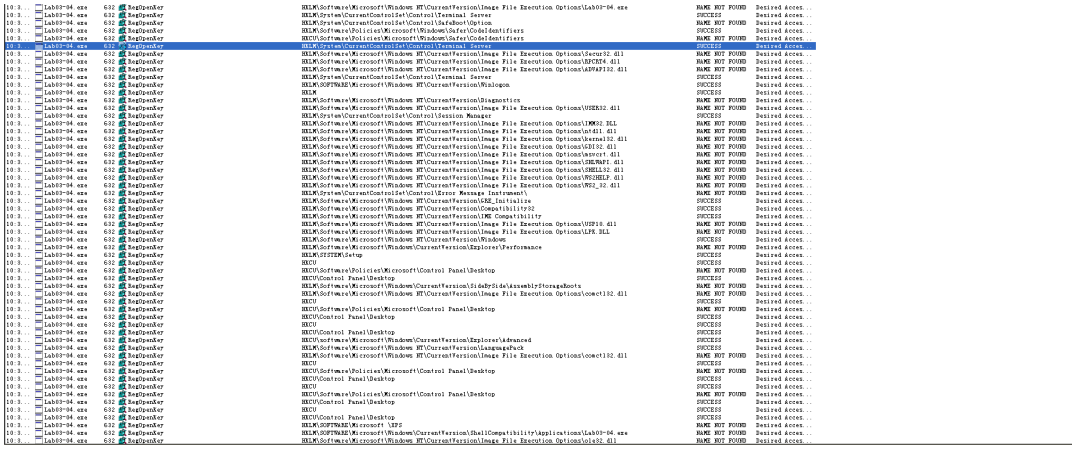
2. 使用动态分析

1. 使用procmon和process explorer工具，监控lab03-04.exe的运行

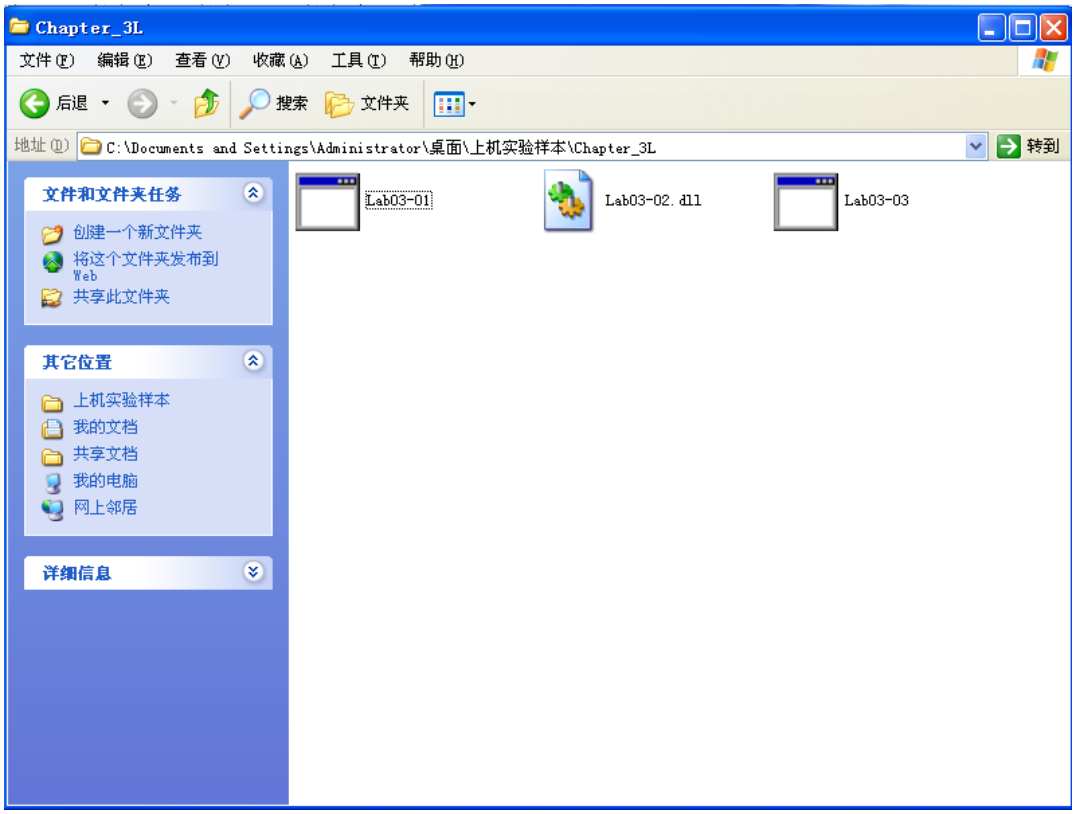


发现程序打开了一个命令行窗口，然后这个窗口很快就关闭了。推测应该是运行方式不对，应该不是双击运行，而是使用命令行的方式运行，而且根据strings分析的结果来看，可能是在运行的时候少了一些参数。

对procmon中的监控进行过滤，得到如下图结果：

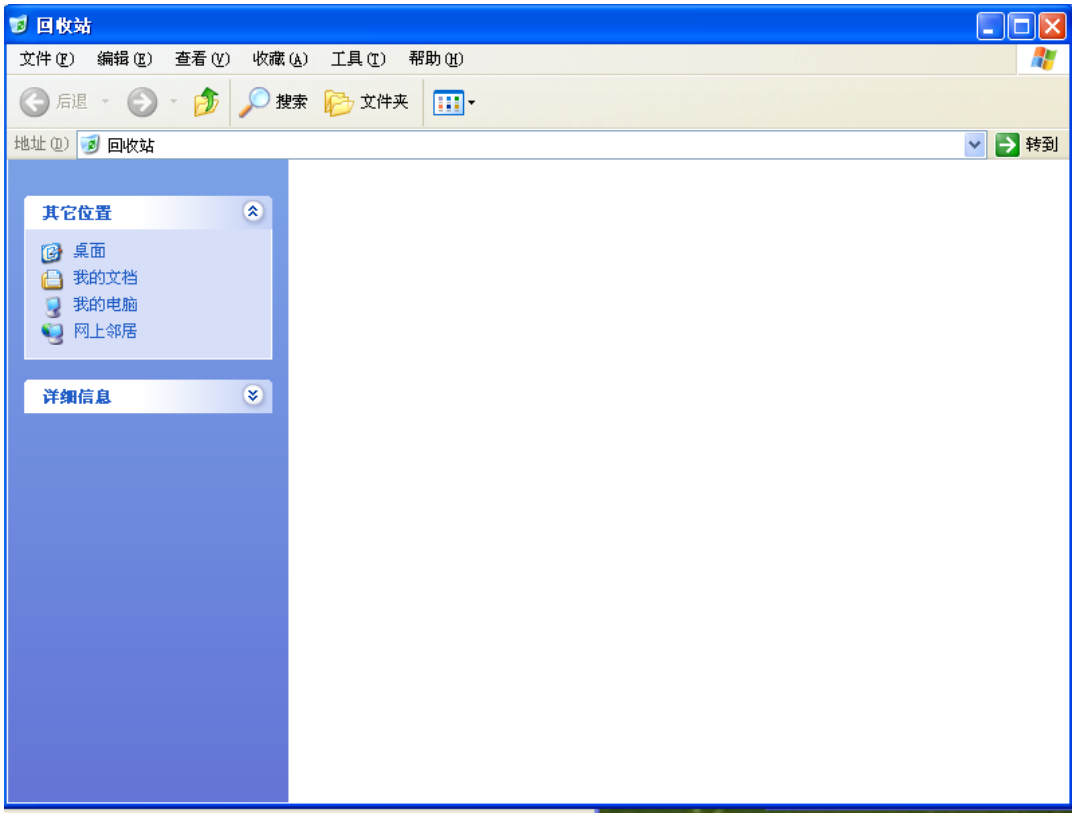


发现Lab03-04.exe执行了大量的对注册表进行修改的操作。



同时在运行完以后发现原本目录下的文件消失了，应当是执行了自我删除

查看回收站



发现回收站里并没有这个文件，应该是彻底删除了

2. 使用Regshot工具查看其对注册表的操作

得到结果如下：

```
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2021/9/30 02:40:32   ,   2021/9/30 02:40:42
Computer: NIRVANA-82C02E1 , NIRVANA-82C02E1
```

```
Username: Administrator , Administrator

----------------------------------
Values added: 2
----------------------------------
HKU\S-1-5-21-776561741-1123561945-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\Qbphzragf naq Frggvatf\Nqzvavfgengbe\桌面\上机实验样本\Puncgre_3Y\Yno03-04.rkr:  01 00 00 00 06 00 00 00 00 DC 76 8D A4 B5 D7 01
HKU\S-1-5-21-776561741-1123561945-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Documents and Settings\Administrator\桌面\上机实验样本\Chapter_3L\Lab03-04.exe: "Lab03-04"

----------------------------------
Values modified: 3
----------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  4A 85 E6 79 51 F7 37 C5 0A 7B 01 FF 8A 60 C1 0C 9D 15 84 65 51 68 46 40 67 6B 11 04 88 80 7A 34 48 13 20 4D 31 AB 1D 76 35 71 19 3D D3 39 06 A2 6D 66 78 F5 8E DD 0F 27 0E 6F 89 15 7C 18 EB F5 AA DD 4B 9C AC DE E9 27 5D C0 E9 E6 90 51 04 70
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  52 AC 01 AE 0A 70 44 C5 B1 AD 74 99 19 5D E5 B2 7C 4A BE D8 D7 5C C6 1E C4 3A C4 0F 7E D7 DC 2C 31 08 8E CC 30 C6 43 C8 55 08 C1 27 97 69 C0 77 01 70 1C 35 1F B0 61 A1 6B B7 14 66 55 9D 9A DD 06 D5 87 6F 04 05 70 D5 97 83 6B DE 4B E7 96 7F
HKU\S-1-5-21-776561741-1123561945-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:  01 00 00 00 0F 00 00 00 50 47 F7 88 A4 B5 D7 01
HKU\S-1-5-21-776561741-1123561945-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:  01 00 00 00 10 00 00 00 00 DC 76 8D A4 B5 D7 01
HKU\S-1-5-21-776561741-1123561945-725345543-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx:  01 00 00 00 02 00 00 00 00 00 00 00 FF FF FF FF
HKU\S-1-5-21-776561741-1123561945-725345543-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx:  02 00 00 00 01 00 00 00 00 00 00 00 FF FF FF FF

----------------------------------
Total changes: 5
----------------------------------
```

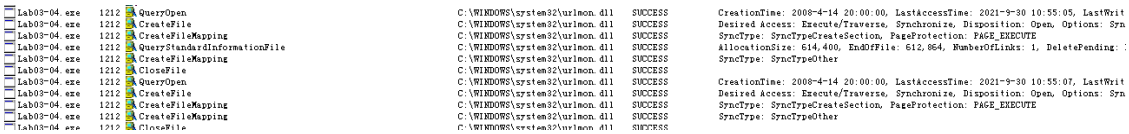
很明显的可以看见这个程序增加了注册表的表项，其中一个比较值得注意的是其增加的位置：`ShellNoRoam\MUICache`，并且后面跟了这个程序的绝对路径，经过查询发现这个键值的作用是：1、防火墙阻止程序名称与实际程序描述不一致时，只能通过注册表更改数值数据信息（如绝对路径不变，即不会建立新的键值时），也可直接删除整个键，系统会重新建立新的键值。2、个性化系统exe名称显示，更改数值数据信息。 如：查找到“回收站”键值更改为“垃圾桶”等。其它程序也可做类似的更改。

3. 通过刚刚过程2的行为结果来看，发现双击运行是存在问题的，所以接下来使用命令行运行的方式重新进行监控、分析，并利用strings中的-in,-cc,-re进行测试。

首先使用-in指令进行测试，因为猜测in是install指令的缩写，可能执行以后的行为特征更加明显

使用procmon和process explorer工具进行监测时发现这个程序依旧是很快就结束了，并且也执行了注册表修改等的操作。

这次进行过滤时，只针对process name进行了过滤，而没有单独筛选对注册表的操作，发现了一些刚刚没有没有发现的对文件的操作。



发现其对urlmon.dll文件有进行操作，从文件的名称就可以推断出这个应该是对网络行为进行监测的一个PE文件。

之后对-cc，-re指令都进行了同样的测试，发现这个程序依旧是会执行自我删除，并且没有表现出更多的行为。

问题回答

Q1

当运行了这个程序以后，会发现程序会将原本目录下的程序文件删除，也就是执行自我删除。

Q2

通过之前strings工具得到的结果和双击运行时出现的cmd窗口猜测，可能双击运行的方式是不正确的，应该是使用命令行的方式运行，并且可能缺少了命令行参数，又或者是干脆少了某些必要的部件。

Q3

根据strings的检测结果来看，这个程序可能的执行方式应当是以命令行的方式进行运行的，并且在运行的时候还需要一定的参数。（但是在根据strings工具检测出的三个参数进行实验时，很不幸的是并没有发现样本的其他特殊行为，猜测可能是样本是用命令行执行，但是还缺少了一些其他的什么的条件，导致样本并没有能够正确的执行）