

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：

```
C:\Windows\System32\cmd.exe

u-
jjjjjj
advpack
hk?
^Pj
<2f
Y
uP
StubPath
SOFTWARE\Classes\http\shell\open\commandU
Software\Microsoft\Active Setup\Installed Components\
test
www.practicalmalwareanalysis.com
admin
VideoDriver
WinUMX32-
vmx32to64.exe
U
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Ph?
U5h
U1
UQÇ
U>Ç
u'Ç
U>U
U
u1Ç
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
PWj
AppData
U1
EW
j0h
UQj
UiW
U%X_
tÇÇ
```

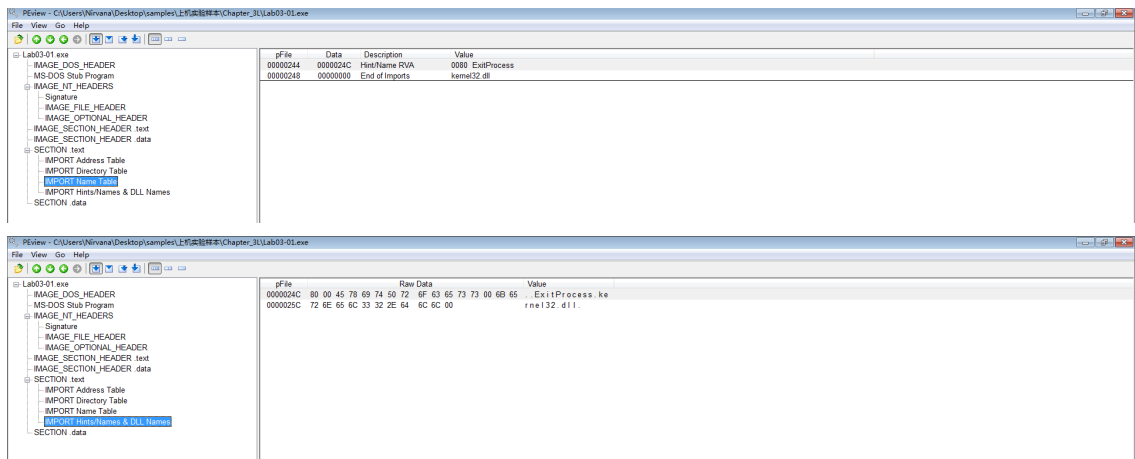
2. 使用PEview工具，得到Import信息如下：

The first screenshot shows the PEview tool with the 'Import Address Table' selected in the left pane. The right pane displays a table with the following data:

pfile	Data	Description	Value
00000200	0000004C	HintName RVA	0000
00000204	00000000	End of Imports	kernel32.dll

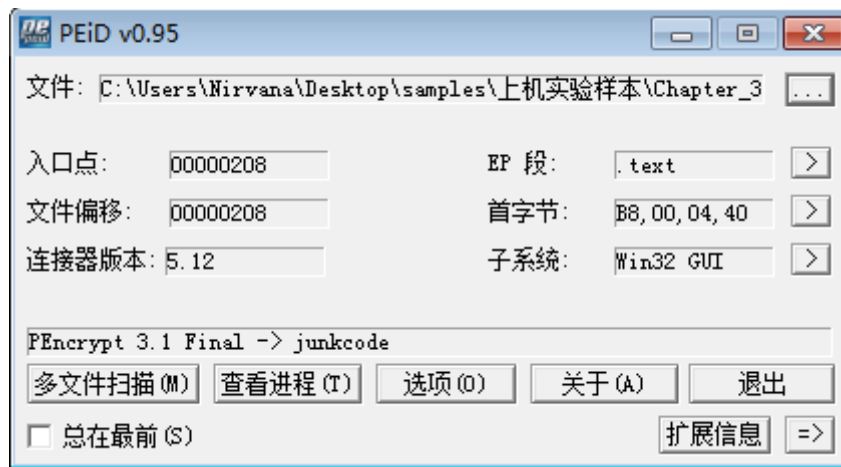
The second screenshot shows the PEview tool with the 'Import Name Table' selected in the left pane. The right pane displays a table with the following data:

pfile	Data	Description	Value
0000021C	00000244	Import Name Table RVA	
00000220	00000000	Time Date Stamp	
00000224	00000000	Forwarder Chain	
00000228	0000025A	Name RVA	kernel32.dll
0000022C	00000200	Import Address Table RVA	
00000230	00000000		
00000234	00000000		
00000238	00000000		
0000023C	00000000		
00000240	00000000		



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。

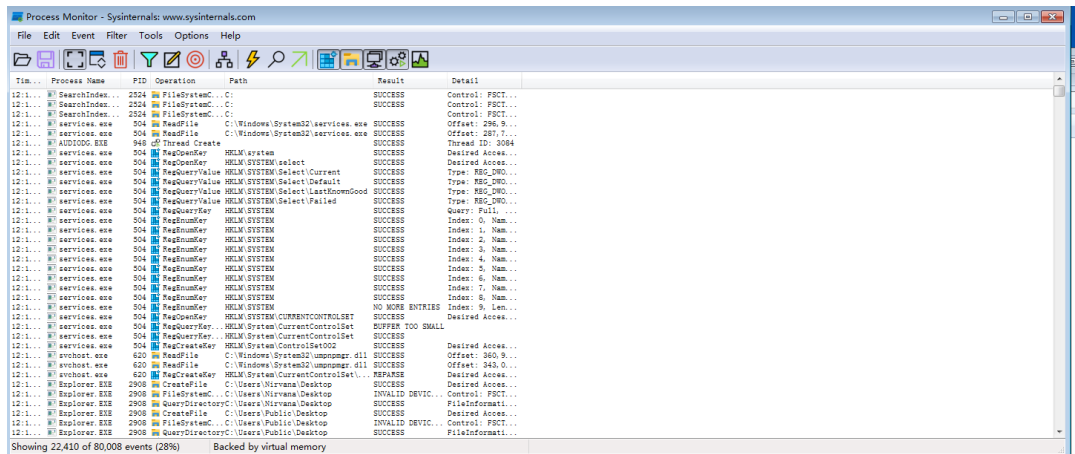
3. 使用PeID工具验证是否有加壳



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：



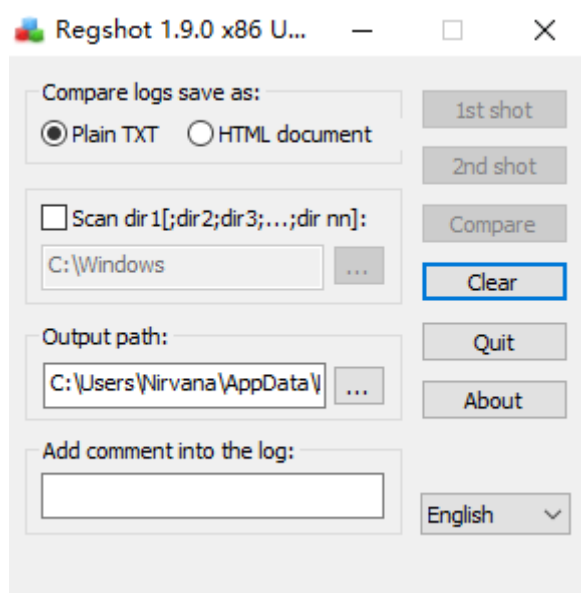
将当前状态进行清空，并运行lab03-01.exe

设置过滤条件为：

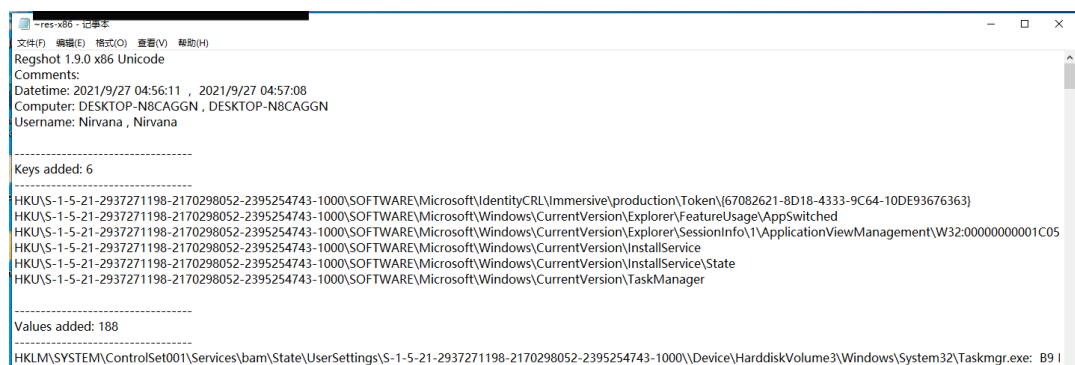
Column	Relation	Value	Action
<input checked="" type="checkbox"/> Process Name	is	lab03-01.exe	Include
<input checked="" type="checkbox"/> Operation	is	RegSetValue	Include
<input checked="" type="checkbox"/> Operation	is	WriteFile	Include

可以查看到当前过滤条件下得到的结果为：

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。

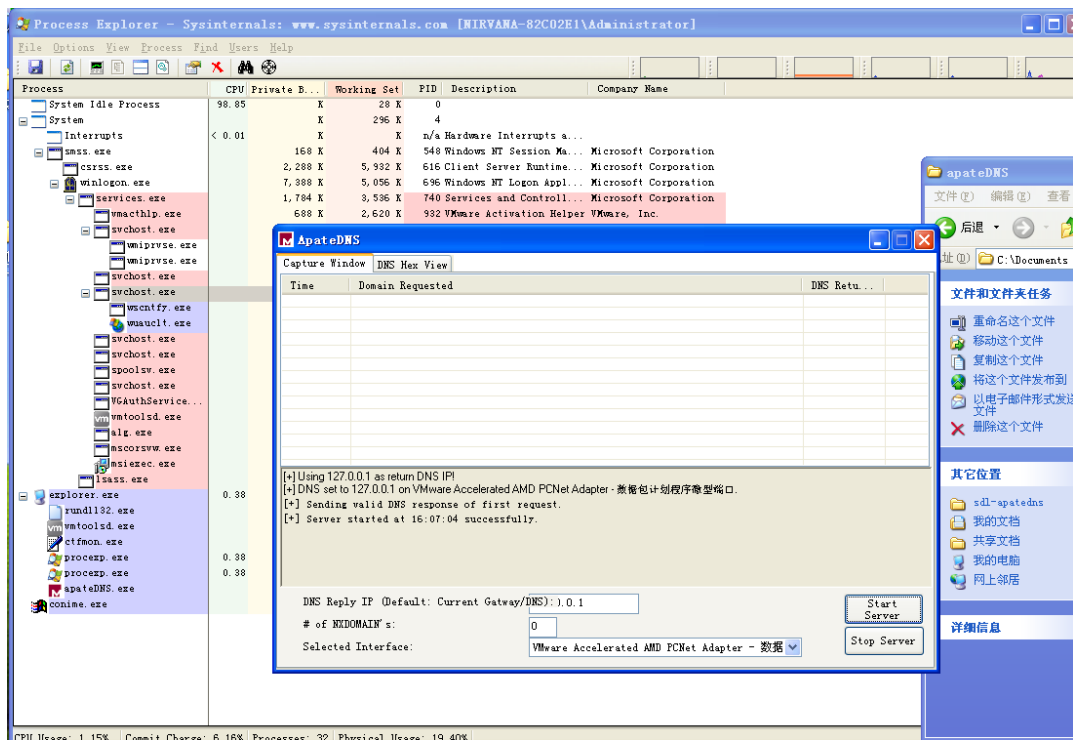
但是在其中有一反馈的信息是： `\Software\Classes\Local`

`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

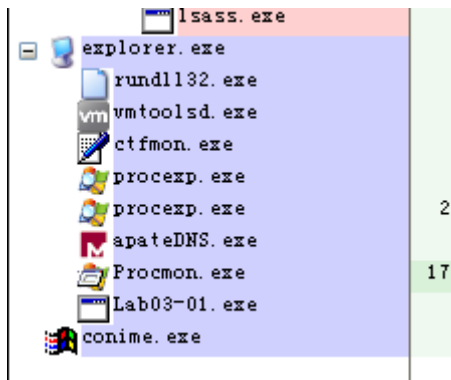
首先启动process explorer和ApateDNS



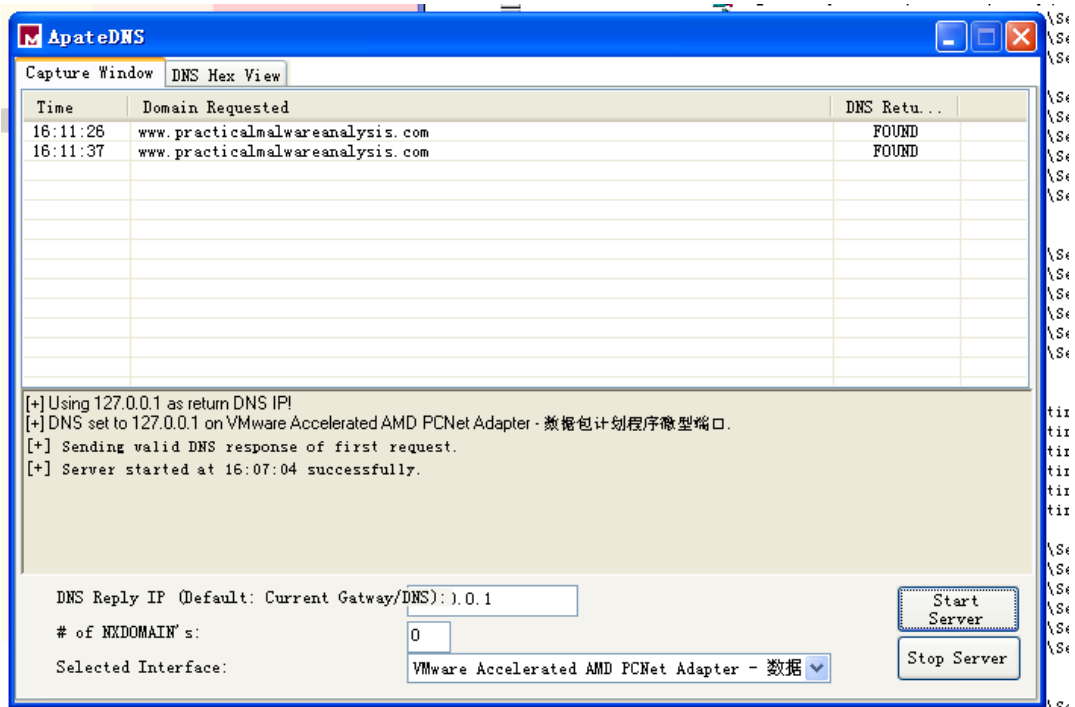
再启动procmon，清空当前状态，重新打开监视

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



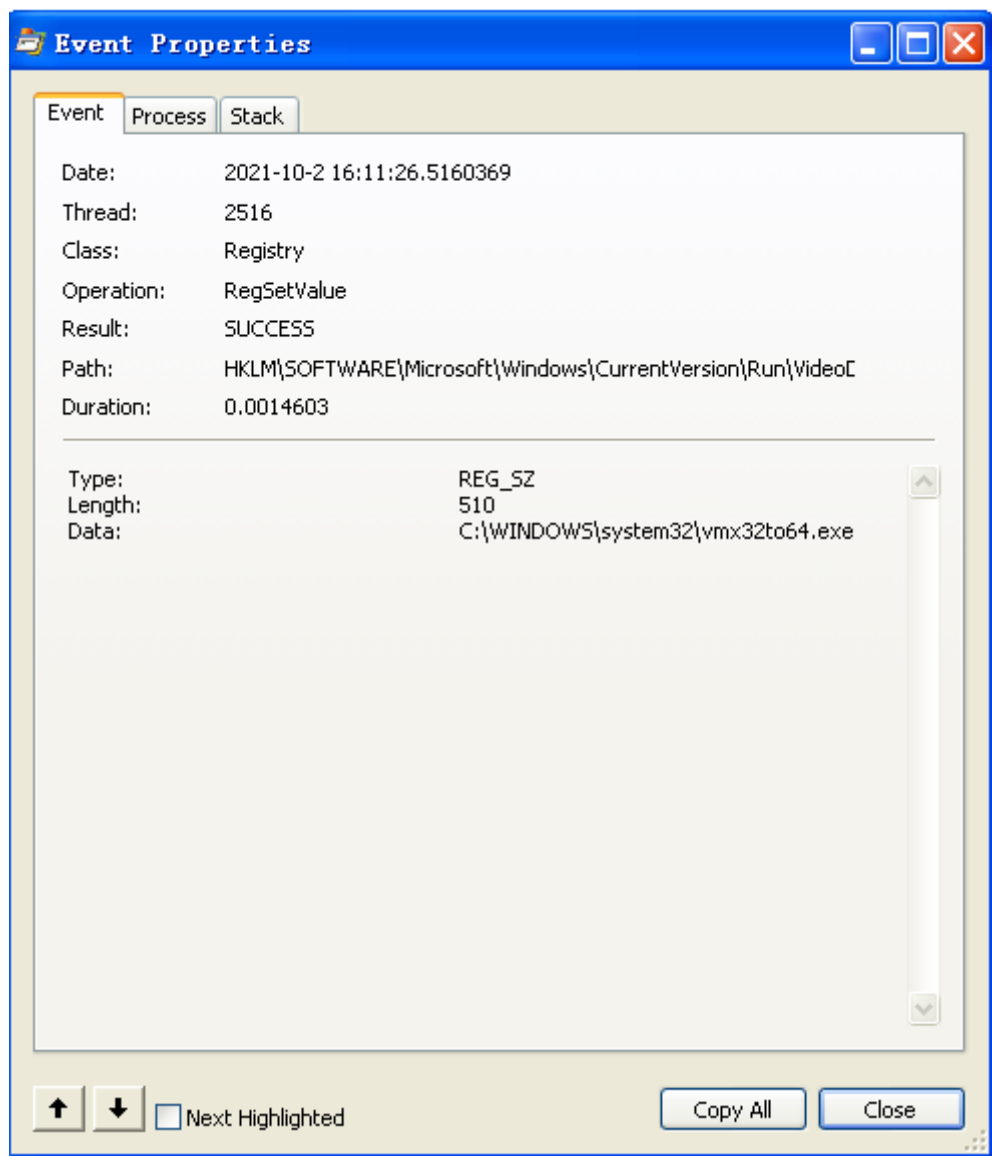
并且在ApatDNS中可以发现存在有网络访问的行为，访问的网址为
www.practicalmalwareanalysis.com



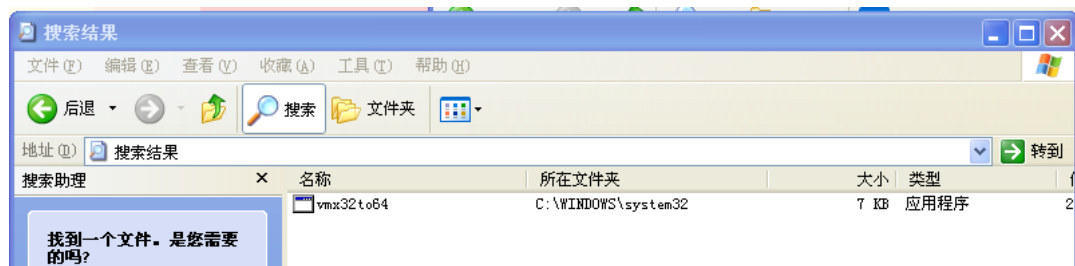
在procmon中设置过滤条件，得到如下图的情况

Time	Process Name	PID	Operation	Path
16:11:26	lab03-01.exe	2528	RegSetValue	HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\RMG\Seed
16:11:26	lab03-01.exe	2528	WriteFile	C:\WINDOWS\system32\vmx32to64.exe
16:11:26	lab03-01.exe	2528	RegSetValue	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\VideoDriver
16:11:26	lab03-01.exe	2528	RegSetValue	HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\RMG\Seed
16:11:26	lab03-01.exe	2528	RegSetValue	HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\RMG\Seed
16:11:26	lab03-01.exe	2528	RegSetValue	HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\RMG\Seed
16:11:26	lab03-01.exe	2528	RegSetValue	HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\RMG\Seed
16:11:26	lab03-01.exe	2528	RegSetValue	HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\RMG\Seed
16:11:26	lab03-01.exe	2528	RegSetValue	HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\RMG\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（原本是想这个是一个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：


```
C:\Documents and Settings\Administrator\桌面\计算机病毒分析工具\netcat-1...
Cmd line: nc -l -p 443
?J?W? 璫y肥k佈赁$BC蔡Z格 L輕枅 h'o鉛?@檢<uQLUz闢?Hy梹?稭 z精?○整忡Q:33囁
得$5I扯>z y SskU!P悞?h=淳 拉δi盤E5t焗'莖脯R徽簞△qWP*樣mG.p背蹇6Lk謾E雖0 ??酸瓊
蜣 ??攪H蜎??R=\弩燁 ←?臺3j?調嬭<9+δ醺?V??岳△啞 S▽沱Qu_
```

```
C:\Documents and Settings\Administrator\桌面\计算机病毒分析工具\netcat-1...
Cmd line: nc -l -p 443
k鬱1荔4噓周?綰1>汜M??崑Qa?DUq店J@?_X廐vK??&▼酯?襖欄He孜gL籥p僊 s<滢萊 <Y0缺?
l^_N?冻BR襪1U 濫??豫攪 畝~4s0络!!a=~?_018_dU龜瞬弭 f厝?Apu?◆?^X始? <1X<梗?<
“~ 木!融???祆攆奢!q>闻0東鴉?H$△>亂A↓標$?▲畜央C肺鉗↓鞘郅H△LU<??:轡灝△&??
```

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

```
GetModuleFileNameA
Sleep
TerminateThread
WaitForSingleObject
GetSystemTime
CreateThread
GetProcAddress
LoadLibraryA
GetLongPathNameA
GetTempPathA
ReadFile
CloseHandle
CreateProcessA
GetStartupInfoA
CreatePipe
GetCurrentDirectoryA
GetLastError
lstrlenA
SetLastError
OutputDebugStringA
KERNEL32.dll
RegisterServiceCtrlHandlerA
RegSetValueExA
RegCreateKeyA
CloseServiceHandle
CreateServiceA
OpenSCManagerA
RegCloseKey
RegQueryValueExA
RegOpenKeyExA
DeleteService
OpenServiceA
SetServiceStatus
ADVAPI32.dll
WSASocketA
WS2_32.dll
InternetReadFile
HttpQueryInfoA
HttpSendRequestA
HttpOpenRequestA
InternetConnectA
InternetOpenA
InternetCloseHandle
WININET.dll
memset
wcstombs
strncpy
strcat
strcpy
atoi
```

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

```

Lab03-02.dll
Install
ServiceMain
UninstallService
installA
uninstallA
Y29ubmVjdA==
practicalmalwareanalysis.com
serve.html
dW5zdXBwb3J0
c2x1ZXA=
Y21k
cXUpdA==
**/*
  Windows XP 6.11
CreateProcessA
kernel32.dll
.exe
GET
HTTP/1.1
%s %s
1234567890123456
quit
exit
getfile
cmd.exe /c
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/-!>
<!--

```

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

```

GetModuleFileName(<) get dll path
Parameters
Type
Start
ObjectName
LocalSystem
ErrorControl
DisplayName
Description
Depends INA+, Collects and stores network configuration and location information
, and notifies applications when this information changes.
ImagePath
%SystemRoot%\System32\svchost.exe -k
SYSTEM\CurrentControlSet\Services\
CreateService(<%) error %d
Intranet Network Awareness (INA+)
%SystemRoot%\System32\svchost.exe -k netsvcs
OpenSCManager(<)
You specify service name not in Svchost\netsvcs, must be one of following:
RegQueryValueEx(Svchost\netsvcs)
netsvcs
RegOpenKeyEx(<%) KEY_QUERY_VALUE success.
RegOpenKeyEx(<%) KEY_QUERY_VALUE error .
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost
IPRIP
uninstall success
OpenService(<%) error 2
OpenService(<%) error 1
uninstall is starting

```

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`。

```
C:\Documents and Settings\Administrator\桌面\上机实验样本\Chapter_3L>rundll32.exe Lab03-02.dll,installA
```

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

explorer.exe	14,212 K	7,440 K	1856 Windows Explorer	Microsoft Corporation
rundll32.exe	2,396 K	3,672 K	324 Run a DLL as an App	Microsoft Corporation

等到rundll程序执行结束后，查看运行前后注册表的变化：

```

1  -----
2  Keys added: 6
3  -----
4  HKLM\SYSTEM\ControlSet001\Services\IPRIP
5  HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters
6  HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security
7  HKLM\SYSTEM\CurrentControlSet\Services\IPRIP
8  HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters
9  HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security
10
11 -----
12 Values added: 21
13 -----
14 HKLM\SYSTEM\ControlSet001\Services\IPRIP\Type: 0x00000020
15 HKLM\SYSTEM\ControlSet001\Services\IPRIP\Start: 0x00000002
16 HKLM\SYSTEM\ControlSet001\Services\IPRIP>ErrorControl: 0x00000001
17 HKLM\SYSTEM\ControlSet001\Services\IPRIP\ImagePath:
18 "%SystemRoot%\System32\svchost.exe -k netsvcs"
19 HKLM\SYSTEM\ControlSet001\Services\IPRIP\DisplayName: "Intranet
20 Network Awareness (INA+)"
21 HKLM\SYSTEM\ControlSet001\Services\IPRIP\ObjectName: "LocalSystem"
22 HKLM\SYSTEM\ControlSet001\Services\IPRIP>Description: "Depends
23 INA+, collects and stores network configuration and location
24 information, and notifies applications when this information
25 changes."
26 HKLM\SYSTEM\ControlSet001\Services\IPRIP\DependOnService: 52 00 70
27 00 63 00 53 00 73 00 00 00 00 00
28 HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters\ServiceDll:
29 "C:\Documents and Settings\Administrator\桌面\上机实验样本
30 \Chapter_3L\Lab03-02.dll"

```

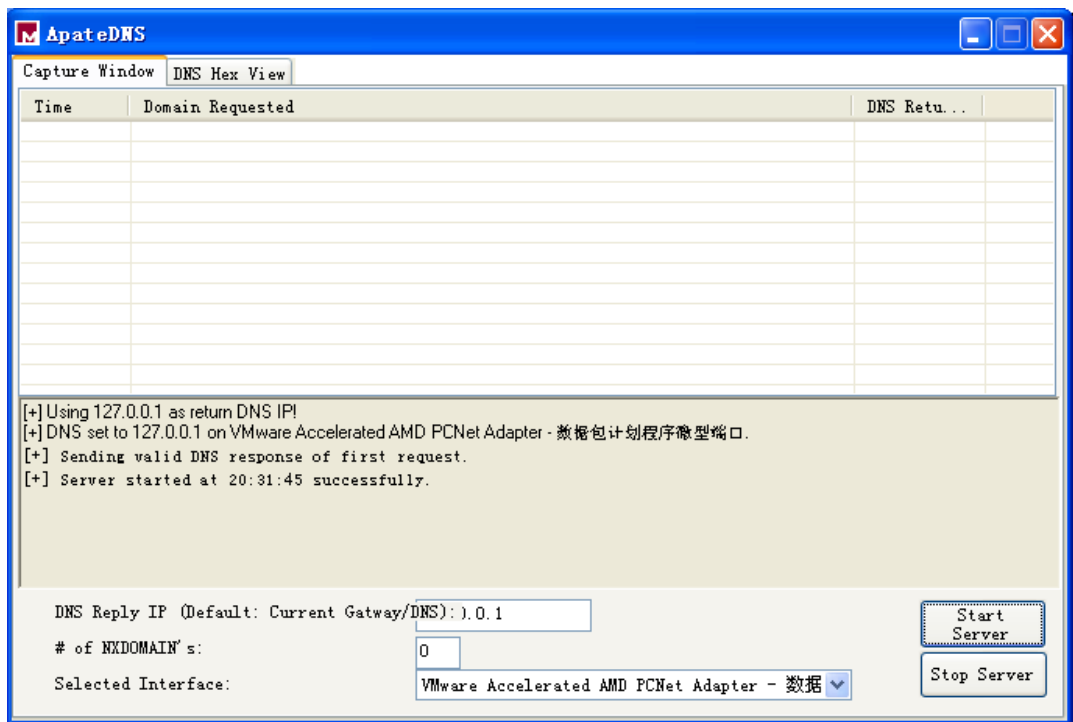
```

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 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 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 18 00 FF 01 0F 00 01 02 00 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 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

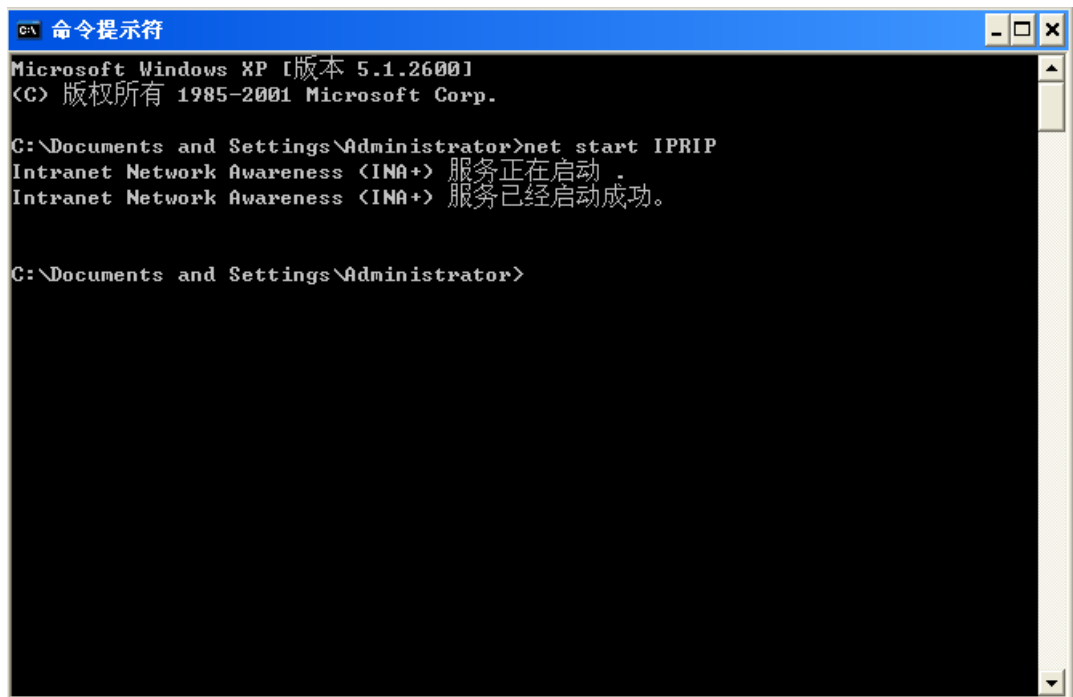
```

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



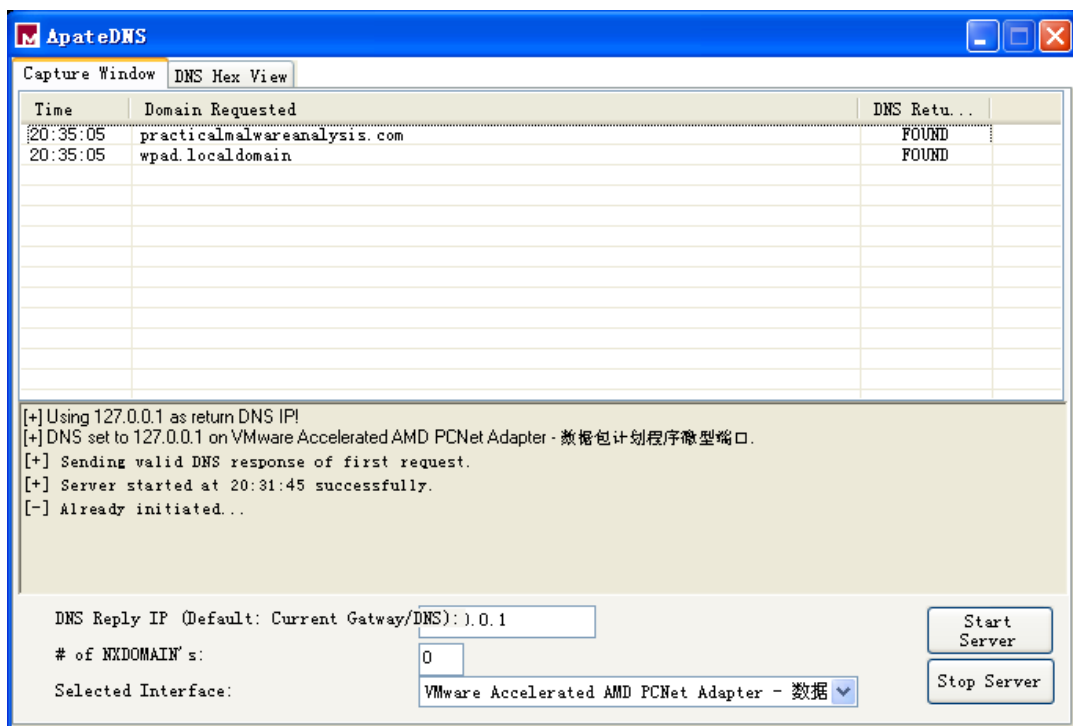
启动服务



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

winlogon.exe	6,972 K	4,672 K	696 Windows NT Logon Appl...	Microsoft Corporation
services.exe	1,760 K	3,520 K	740 Services and Controll...	Microsoft Corporation
vmacthlp.exe	688 K	2,620 K	932 VMware Activation Helper	VMware, Inc.
svchost.exe	3,060 K	4,908 K	948 Generic Host Process ...	Microsoft Corporation
vmtoolsd.exe	3,600 K	8,308 K	1764 VMI	Microsoft Corporation
svchost.exe	1,992 K	4,588 K	1016 Generic Host Process ...	Microsoft Corporation
svchost.exe	19,364 K	28,932 K	1160 Generic Host Process ...	Microsoft Corporation
wscntfy.exe	668 K	2,520 K	1448 Windows Security Cent...	Microsoft Corporation
wuauclt.exe	5,768 K	5,456 K	3252 Automatic Updates	Microsoft Corporation
svchost.exe	1,300 K	3,628 K	1272 Generic Host Process ...	Microsoft Corporation
svchost.exe	1,764 K	4,532 K	1340 Generic Host Process ...	Microsoft Corporation
spoolsv.exe	4,480 K	7,732 K	1504 Spooler SubSystem App	Microsoft Corporation
svchost.exe	2,256 K	3,376 K	180 Generic Host Process ...	Microsoft Corporation
VGAAuthService...	6,292 K	9,148 K	472 VMware Guest Authent...	VMware, Inc.
vmtoolsd.exe	11,592 K	14,716 K	636 VMware Tools Core Ser...	VMware, Inc.
alg.exe	1,260 K	3,704 K	1780 Application Layer Gat...	Microsoft Corporation
mscorsvw.exe	1,368 K	4,048 K	2928 .NET Runtime Optimiza...	Microsoft Corporation
lsass.exe	4,052 K	6,496 K	752 LSA Shell (Export Ver...	Microsoft Corporation
explorer.exe	13,548 K	7,008 K	1740 Windows Explorer	Microsoft Corporation

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\netc
at-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?

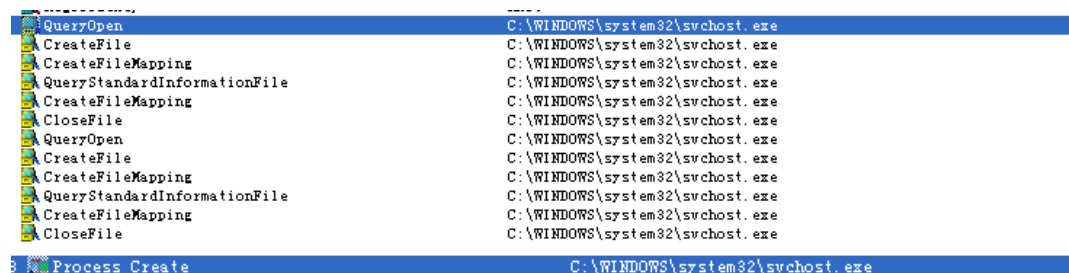
实验过程

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

```
AiY
A34/5<,$a$33.3aAALKAA
a$33.3LKAAA
a$33.3LKAAAA
a$33.3LKAA
wqsyLKla4/ #- $a5.a</<5< -< ;$a>$ 1LKAAAA
wqsvLKla/.5a$/ .4&>a21 "$a'.3a-.6<.a</<5< -< ; 5<./LKAAAA
wqswLKla/.5a$/ .4&>a21 "$a'.3a25< .a</<5< -< ; 5<./LKAAAA
wqstLKla143$a7<354 -a'4/"5<./a" --LKAAA
wqsuLKla/.5a$/ .4&>a21 "$a'.3a
./ $9<5n 5$9<5a5 #- $LKAAAA
wqpxLKla4/ #- $a5.a.1$/a"./2.- $a%$7<"$LKAAAA
wqpyLKla4/$91$ "5$%a>$ 1a$33.3LKAAAA
wqpLKla4/$91$ "5$%a,4-5<5>3$ %a-."*a$33.3LKAAAA
wqpLKla/.5a$/ .4&>a21 "$a'.3a5>3$ %a% 5 LKALK #/.3, -a13.&3 ,a5$3,</ 5<./LKAAAA
wqpxLKla/.5a$/ .4&>a21 "$a'.3a$/7<3./, $/5LKA
wqpyLKla/.5a$/ .4&>a21 "$a'.3a 3&4,$/52LKAAA
wqqsLKla'-. 5</&a1.</5a/.5a-. %$%LKAAAA
<"3.2.'5a
```


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：

Lab03-03.exe	0.38	280 K	1,088 K	3348	
svchost.exe	0.77	1,008 K	2,596 K	3356 Generic Host Process ...	Microsoft Corporation
conime.exe		1,552 K	8,372 K	552 Console IME	Microsoft Corporation

一段时间后：

svchost.exe		1,008 K	2,596 K	3356 Generic Host Process ...	Microsoft Corporation
conime.exe		1,552 K	8,372 K	552 Console IME	Microsoft Corporation

2. 在磁盘上找到创建的svchost.exe这个程序的文件

名称	所在文件夹	大小	类型
svchost	C:\WINDOWS\system32	14 KB	应用程序

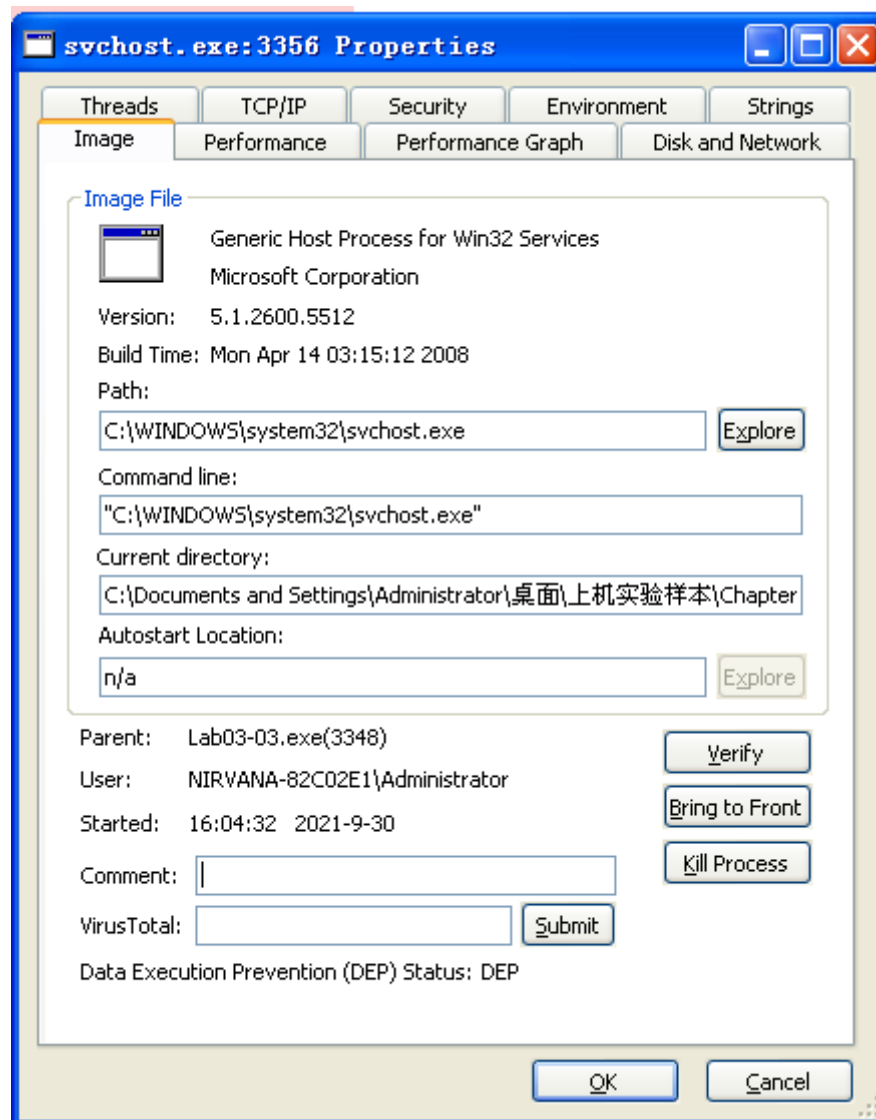
发现这个程序的源文件大小只有14KB

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

svchost.exe	1,008 K	2,632 K	3356 Generic Host Process for Win32 Services	Microsoft Corporation
-------------	---------	---------	--	-----------------------

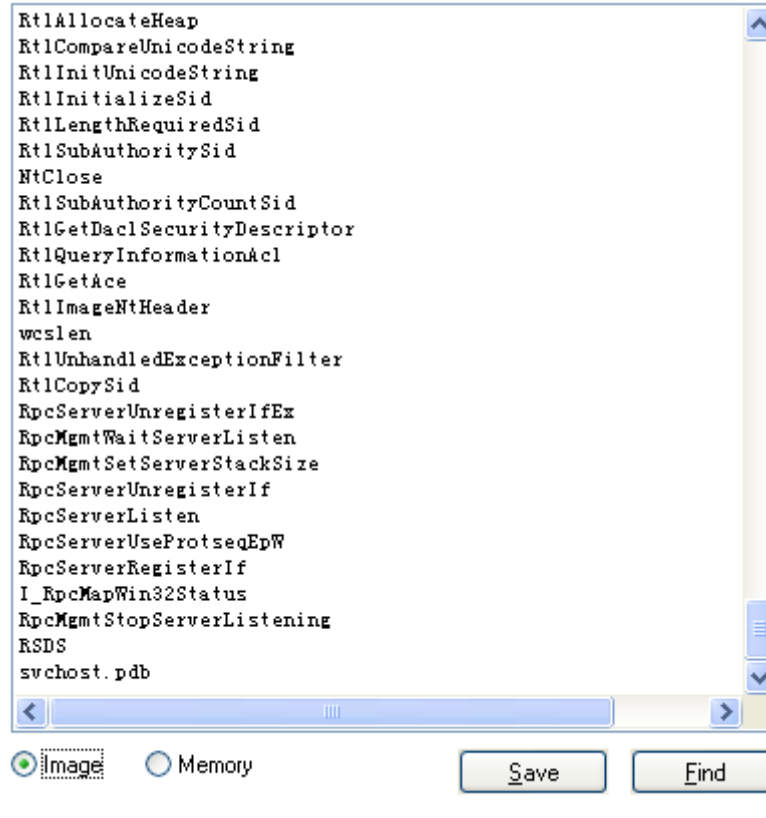
右键-properties，可以看到如下信息：



查看strings中在images和memory分别是什么样的

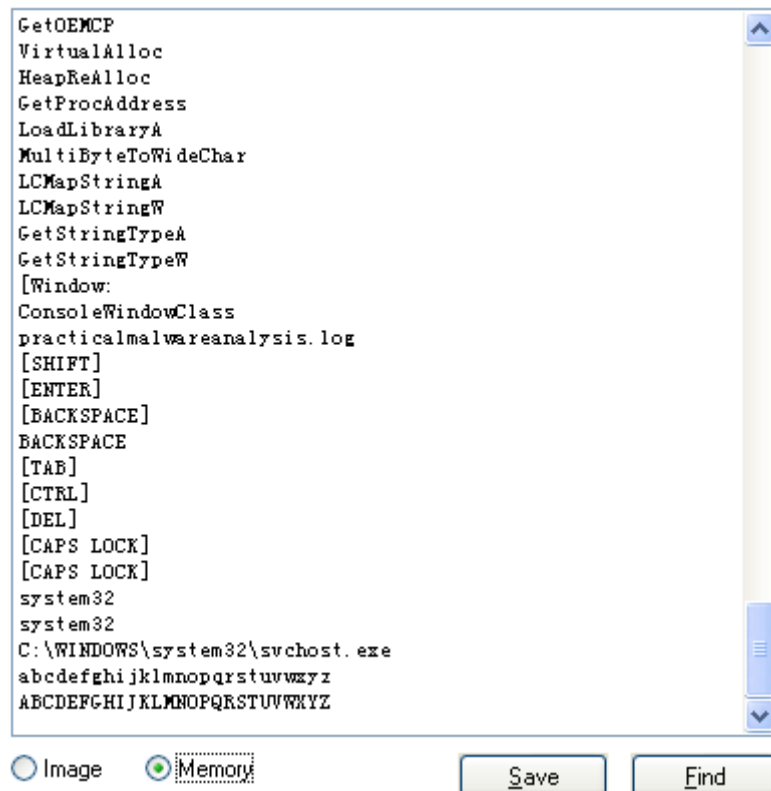
images中:

Printable strings found in the scan:



memory中:

Printable strings found in the scan:



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

```
GLOBAL_HEAP_SELECTED
MSVCRT_HEAP_SELECT
runtime error
TLOSS error
SING error
DOMAIN error
R6028
- unable to initialize heap
R6027
- not enough space for lowio initialization
R6026
- not enough space for stdio initialization
R6025
- pure virtual function call
R6024
- not enough space for _onexit/atexit table
R6019
- unable to open console device
R6018
- unexpected heap error
R6017
- unexpected multithread lock error
R6016
- not enough space for thread data
abnormal program termination
R6009
- not enough space for environment
R6008
- not enough space for arguments
R6002
- floating point not loaded
Microsoft Visual C++ Runtime Library
Runtime Error!
Program:
...
```

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

```
Program name: unknown
SunMonTueWedThuFriSat
JanFebMarAprMayJunJulAugSepOctNovDec
.com
.bat
.cmd
..
```

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

```
GetLastActivePopup
GetActiveWindow
MessageBoxA
user32.dll
PATH
\p`p
pp
CloseHandle
SetFileTime
GetFileTime
CreateFileA
GetSystemDirectoryA
GetLastError
ReadFile
WriteFile
Sleep
GetShortPathNameA
GetModuleFileNameA
CopyFileA
ExpandEnvironmentStringsA
DeleteFileA
KERNEL32.dll
RegQueryValueExA
RegOpenKeyExA
RegSetValueExA
RegCreateKeyExA
RegDeleteValueA
CreateServiceA
CloseServiceHandle
ChangeServiceConfigA
OpenServiceA
OpenSCManagerA
DeleteService
ADVAPI32.dll
ShellExecuteA
SHELL32.dll
WS2_32.dll
ExitProcess
TerminateProcess
GetCurrentProcess
GetTimeZoneInformation
GetSystemTime
GetLocalTime
DuplicateHandle
GetCommandLineA
GetVersion
SetStdHandle
GetFileType
SetHandleCount
GetStdHandle
GetStartupInfoA
```

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。


```

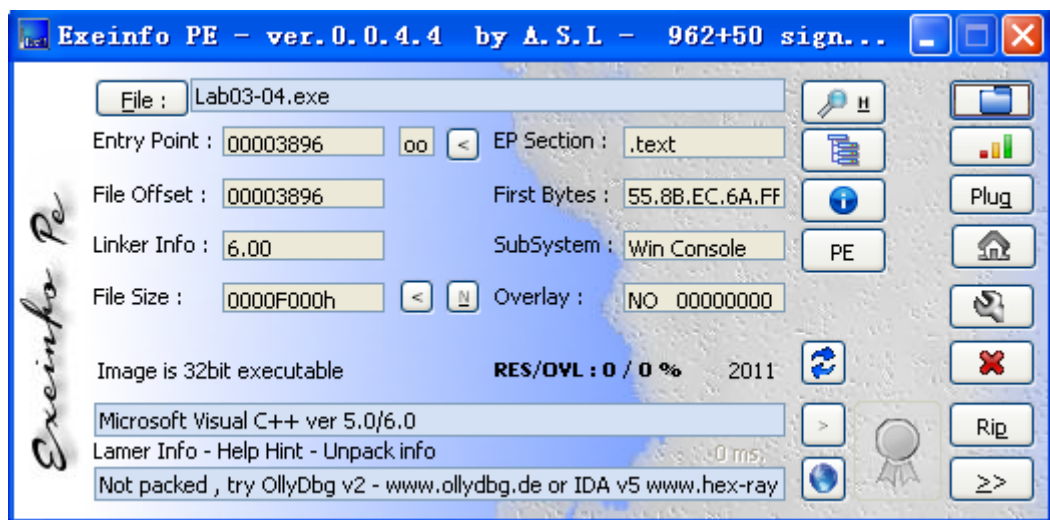
HTTP/1.0
GET
...
...
NOTHING
CMD
DOWNLOAD
UPLOAD
SLEEP
cmd.exe
>> NUL
/c del
ups
http://www.practicalmalwareanalysis.com
Manager Service
.exe
%SYSTEMROOT%\system32\
k:%s h:%s p:%s per:%s
-cc
-re
-in

```

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.practicalmalwareanalysis.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。

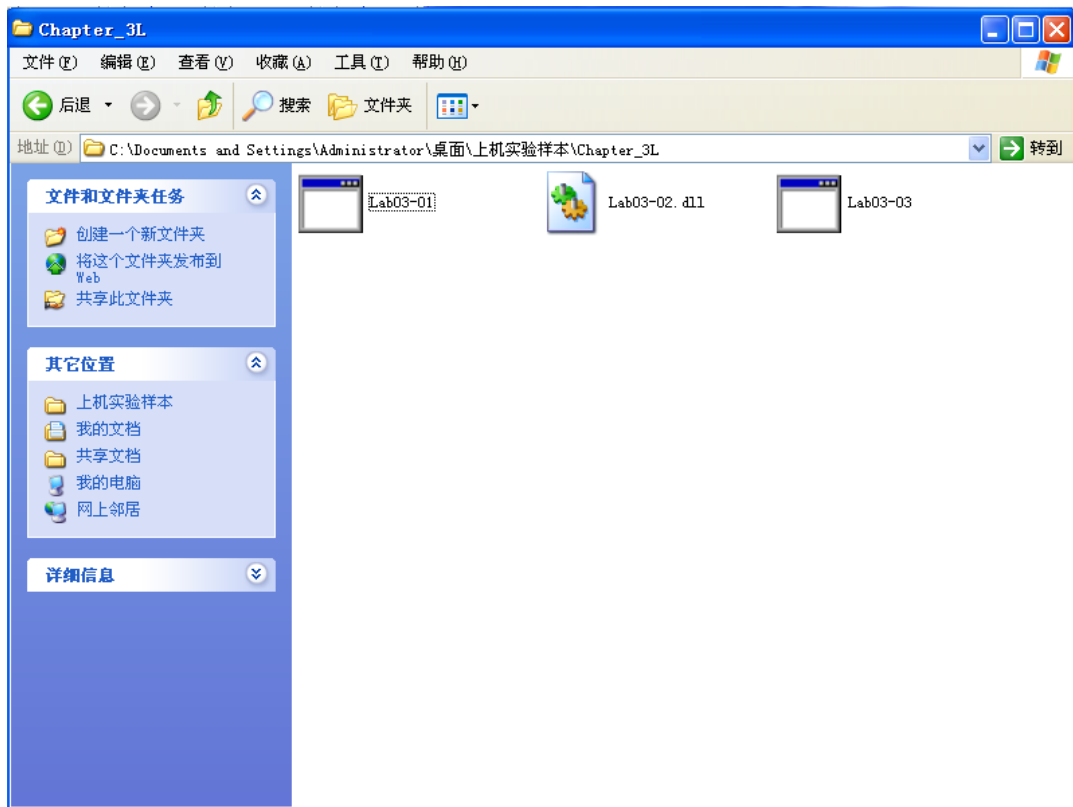
2. 查看是否存在加壳

使用Exeinfo工具查看

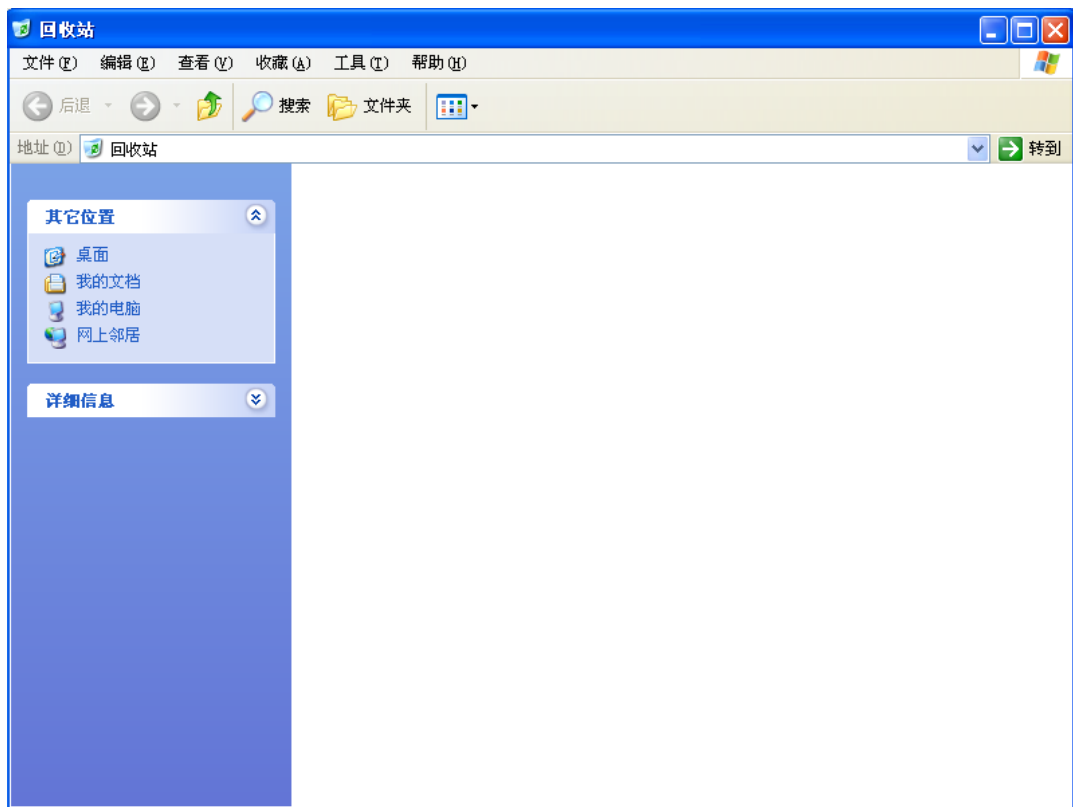


发现此程序确实是没有进行加壳的

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：

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

```

5 Username: Administrator , Administrator
6
7 -----
8 Values added: 2
9 -----
10 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
11 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"
12
13 -----
14 Values modified: 3
15 -----
16 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
17 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
18 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
19 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
20 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
21 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
22
23 -----
24 Total changes: 5
25 -----

```

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

```
C:\Documents and Settings\Administrator\桌面\上机实验样本\Chapter_3L>Lab03-04.exe -in
```

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发现的文件的操作。

Lab03-04.exe	1212	QueryOpen	C:\WINDOWS\system32\urlmon.dll	SUCCESS	CreationTime: 2008-4-14 20:00:00, LastAccessTime: 2021-9-30 10:55:05, LastWriteTime: 2008-4-14 20:00:00, Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Syn
Lab03-04.exe	1212	CreateFile	C:\WINDOWS\system32\urlmon.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE
Lab03-04.exe	1212	CreateFileMapping	C:\WINDOWS\system32\urlmon.dll	SUCCESS	AllocationSize: 614,400, EndOfFile: 612,864, NumberOfLinks: 1, DeletePending: :
Lab03-04.exe	1212	QueryStandardInformationFile	C:\WINDOWS\system32\urlmon.dll	SUCCESS	SyncType: SyncTypeOther
Lab03-04.exe	1212	CreateFileMapping	C:\WINDOWS\system32\urlmon.dll	SUCCESS	
Lab03-04.exe	1212	CloseFile	C:\WINDOWS\system32\urlmon.dll	SUCCESS	
Lab03-04.exe	1212	QueryOpen	C:\WINDOWS\system32\urlmon.dll	SUCCESS	CreationTime: 2008-4-14 20:00:00, LastAccessTime: 2021-9-30 10:55:07, LastWriteTime: 2008-4-14 20:00:00, Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Syn
Lab03-04.exe	1212	CreateFile	C:\WINDOWS\system32\urlmon.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE
Lab03-04.exe	1212	CreateFileMapping	C:\WINDOWS\system32\urlmon.dll	SUCCESS	AllocationSize: 614,400, EndOfFile: 612,864, NumberOfLinks: 1, DeletePending: :
Lab03-04.exe	1212	CreateFileMapping	C:\WINDOWS\system32\urlmon.dll	SUCCESS	SyncType: SyncTypeOther
Lab03-04.exe	1212	CloseFile	C:\WINDOWS\system32\urlmon.dll	SUCCESS	

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）