南開大學

恶意代码分析与防治技术课程实验报告

实验三

学　　院　网络空间安全学院

专　　业　信息安全

学　　号　2213041

姓　　名　李雅帆

班　　级　信安班

一、实验目的

通过静态与动态分析技术，研究恶意软件的行为与特征，包括识别其导入库和功能，监控文件操作、注册表修改和网络通信，分析其作为 Windows 服务的持久性机制，比较内存与磁盘镜像以检测潜在的恶意活动，以及探索自毁特性和分析过程中的复杂性。通过这些研究，为理解和应对恶意软件威胁提供基础。

二、实验原理

1.静态与动态分析：

（1）静态分析：通过检查恶意软件的 PE 文件结构，发现其仅导入了 kernel32.dll，并识别出一些关键字符串，包括注册表路径和域名。这为理解其潜在功能提供了线索。

（2）动态分析：配置了 Process Explorer、Procmon、ApateDNS 等工具，监控文件系统和注册表的变化。在 Process Explorer 中观察到恶意软件创建了名为 WinVMX32 的互斥体，并动态加载了其他 DLL，显示出其网络能力。Procmon 记录了文件复制到 C:/WINDOWS/system32/vmx32to64.exe 的过程，并创建了启动项。

2.恶意服务安装与持久性：

（1）通过运行 rundll32.exe，执行恶意 DLL（如 Lab03-02.dll）中的特定导出函数，将恶意软件作为 Windows 服务安装。这允许其在系统启动时自动运行，服务名称为 IPRIP。

（2）使用 Process Explorer 识别托管该服务的 svchost.exe 进程，并通过 Procmon 监视与恶意软件进程相关的活动。恶意软件通过注册表（HKLM\SYSTEM\CurrentControlSet\Services\IPRIFP\Parameters\ServiceDll）添加自身，确保持久性。

3.内存与磁盘一致性检查：

（1）通过比较内存镜像和磁盘镜像，发现内存中存在特定字符串（如 practicalmalwareanalysis.log），而磁盘镜像中没有。这种不一致性用于检测恶意活动。

（2）恶意软件替换系统进程 svchost.exe，以在系统中运行自身代码，并创建日志文件记录系统活动。此外，恶意软件启动了键盘记录器，窃取用户输入的信息，可能包括敏感数据如密码。

4.自毁特性与复杂性：

（1）在实验中观察到某些恶意软件具有自毁特性，即在运行后立即删除自身。研究人员怀疑这可能需要特定的命令行参数或组件，进行多次尝试但未成功。

（2）这一特性强调了恶意软件分析的挑战，表明深入分析和探索其真正功能的重要性，可能需要更复杂的逆向工程技术。

三、实验过程

• Lab 3-1

使用动态分析基础技术来分析在 Lab03-01.exe 文件中发现的恶意代码。

1. 找出这个恶意代码的导入函数与字符串列表?

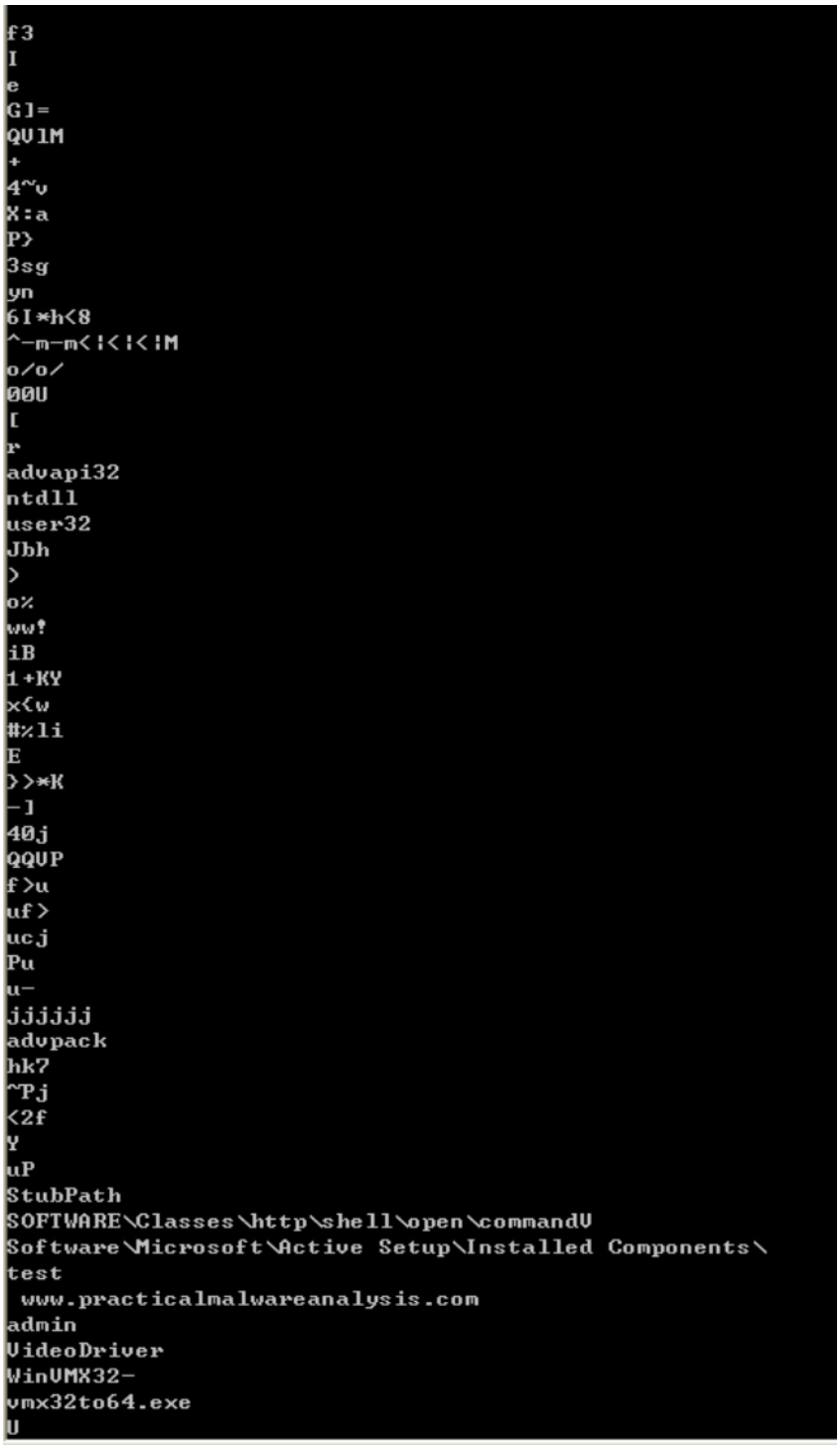
使用 PEiD 查壳，发现加壳，壳为 PEncrypt 3.1 Final -> junkcode。

使用命令 strings Lab03-01.exe 查看可打印字符串，导入函数及字符串列表如下：

```
C:\Documents and Settings\fan\桌面\计算机病毒分析工具\Strings>strings Lab03-01.e
xe

Strings v2.51
Copyright (C) 1999-2013 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
nnn
qn
Nn
Rich
.text
`.data
ExitProcess
kernel32.dll
`3

ws2_32
A)!
_^_
"p7
h
u8
u1Ç
u<
cks=u
ttp=
cks=
CONNECT %s:%i HTTP/1.0
QSRW
?503
200
PWW
thj@h
V!
WMV
PWW
```

```
U
jj
a3
uaE
U
VSWRQ
E^E
YZ_[^
W2

f5
f
u
^E
YZ_[^
G
z
Ls
V
D$0
D$0
D$0
D$0
D$0
D$0
!$,
D$0
t$,
D$0
t$,
!$,
```

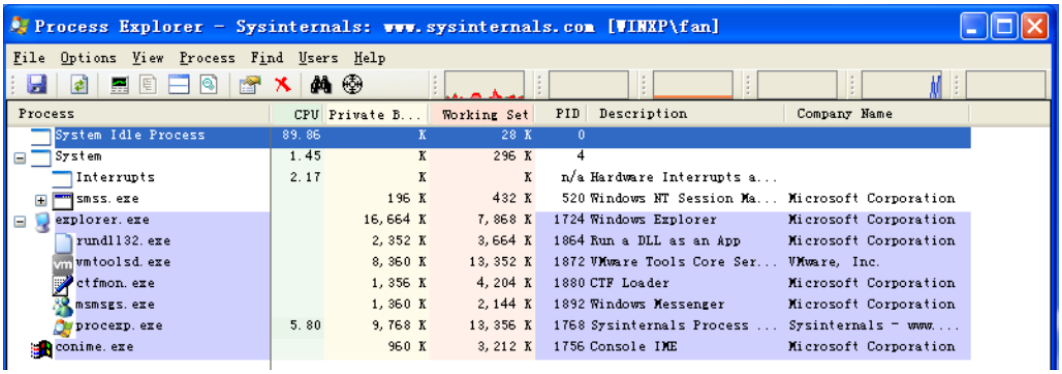

D$4
D$4
D$4
D$4
D$4
D$4
D$4
D$4
D$4
D$4


f3
I
e
G]=
QV1M
+
4^v
X:a
P>
3sg
yn
6I*h<8
^-m-m<¦<¦<¦M
o/o/
00U
[
r
advapi32
ntdll
user32
Jbh
>
o%
ww!
iB
1+KY
x<w
#%1i
E
>>*K
-]
40j
QQVP
f>u
uf>
ucj
Pu
u-
jjjjjj
advpack
hk7
^Pj
<2f
Y
uP
StubPath
SOFTWARE\Classes\http\shell\open\commandV
Software\Microsoft\Active Setup\Installed Components\
test
www.practicalmalwareanalysis.com
admin
VideoDriver
WinVMX32-
vmx32to64.exe
U

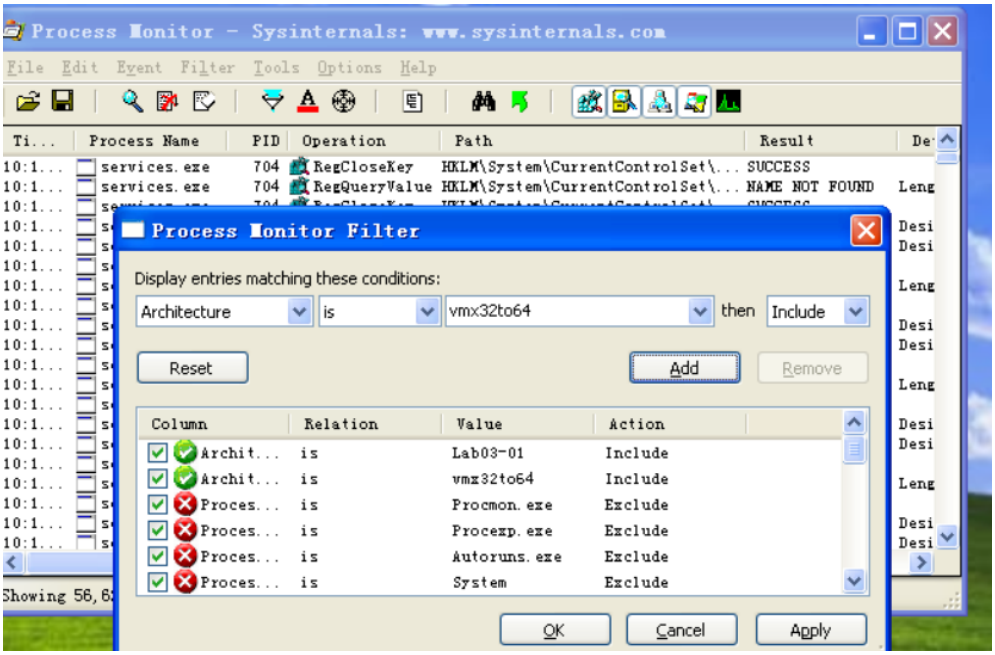
```
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Ph?
V5h
V1
VQÇ
V>Ç
u'Ç
V>V
V
u1Ç
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
PWj
AppData
V1
EW
j@h
VQj
ViW
V%X_
t<Ç
```

2. 这个恶意代码在主机上的感染迹象特征是什么?

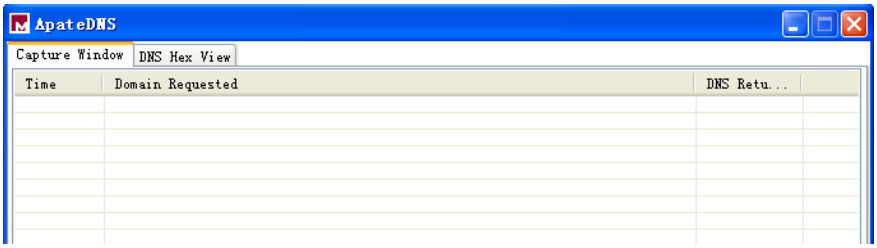
开启 Process Explorer，监视进程运行情况。



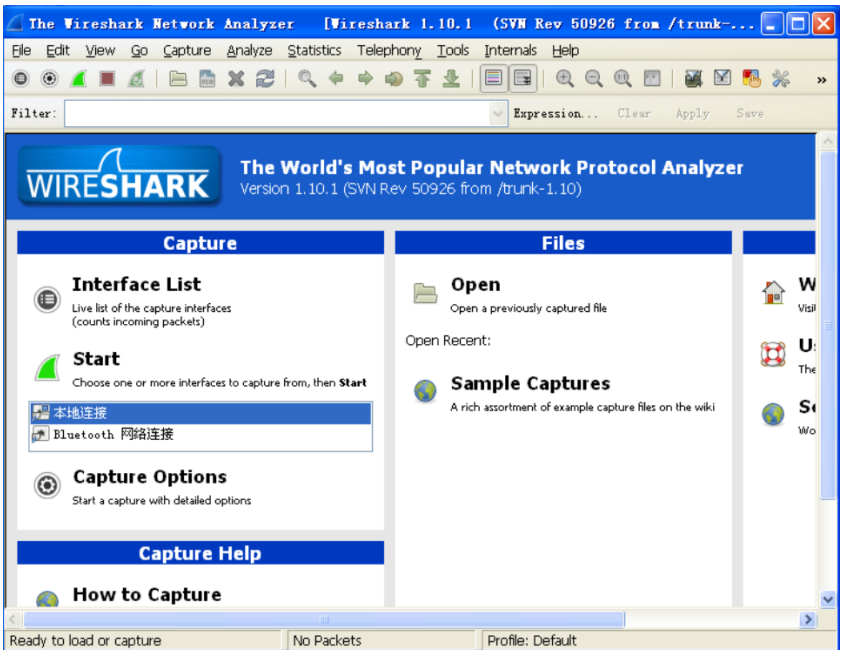
开启 Process Monitor，设置过滤器，通过 strings.exe 看到了一个可疑字符串“vmx32to64.exe”，而该恶意代码名为“Lab03-01.exe”，设置 Lab03-01.exe、vmx32to64 两个过滤器。



开启 ApateDNS，点击“Start Server”监视 DNS 查询请求

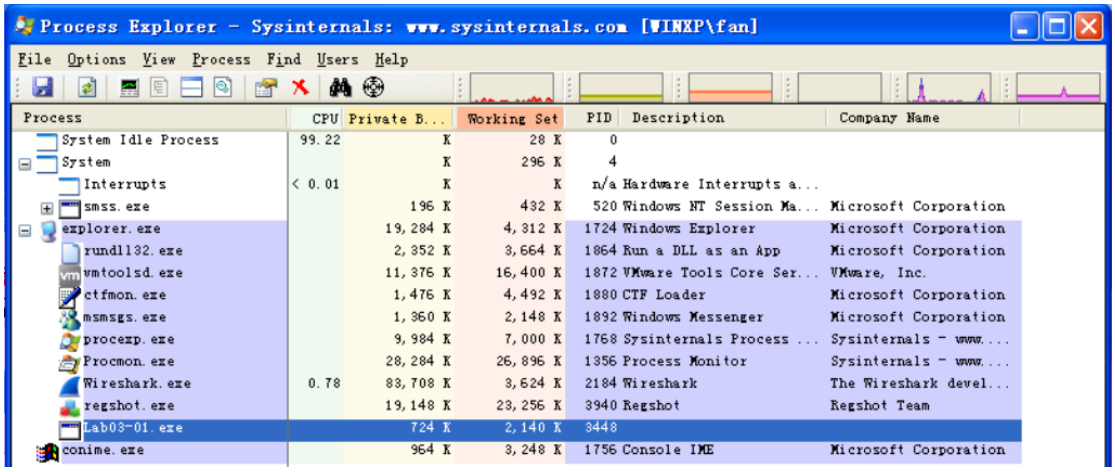


开启 Wireshark 监视网络流量包。

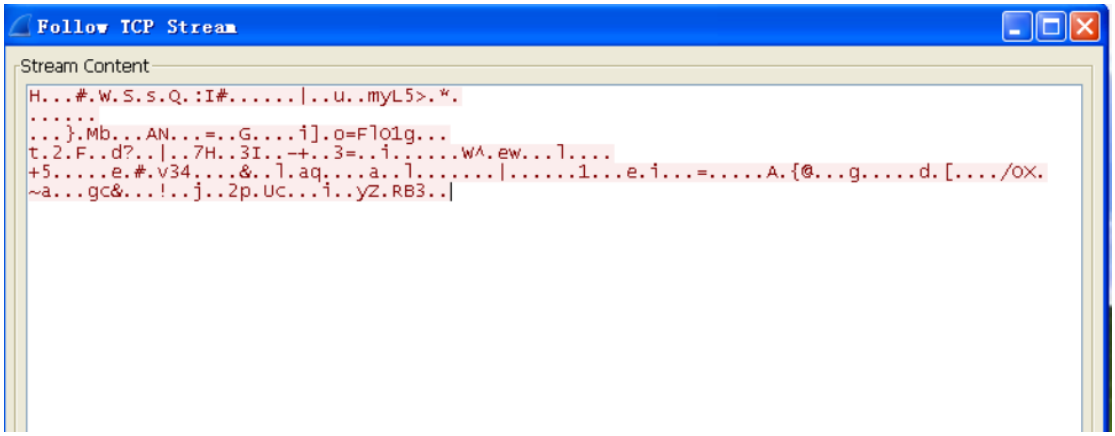


开启 Regshot ，点击“建立快照 A”拍摄运行恶意代码前的快照。

运行 Lab03-01.exe 并查看 ProcessExplorer，观察 Lab03-01.exe 是否在运行，图中我们能够看到 Lab03-01.exe 已经在运行。



在 Wireshark 中右键 TCP 包，点击“跟随 TCP 流”，内容如下。



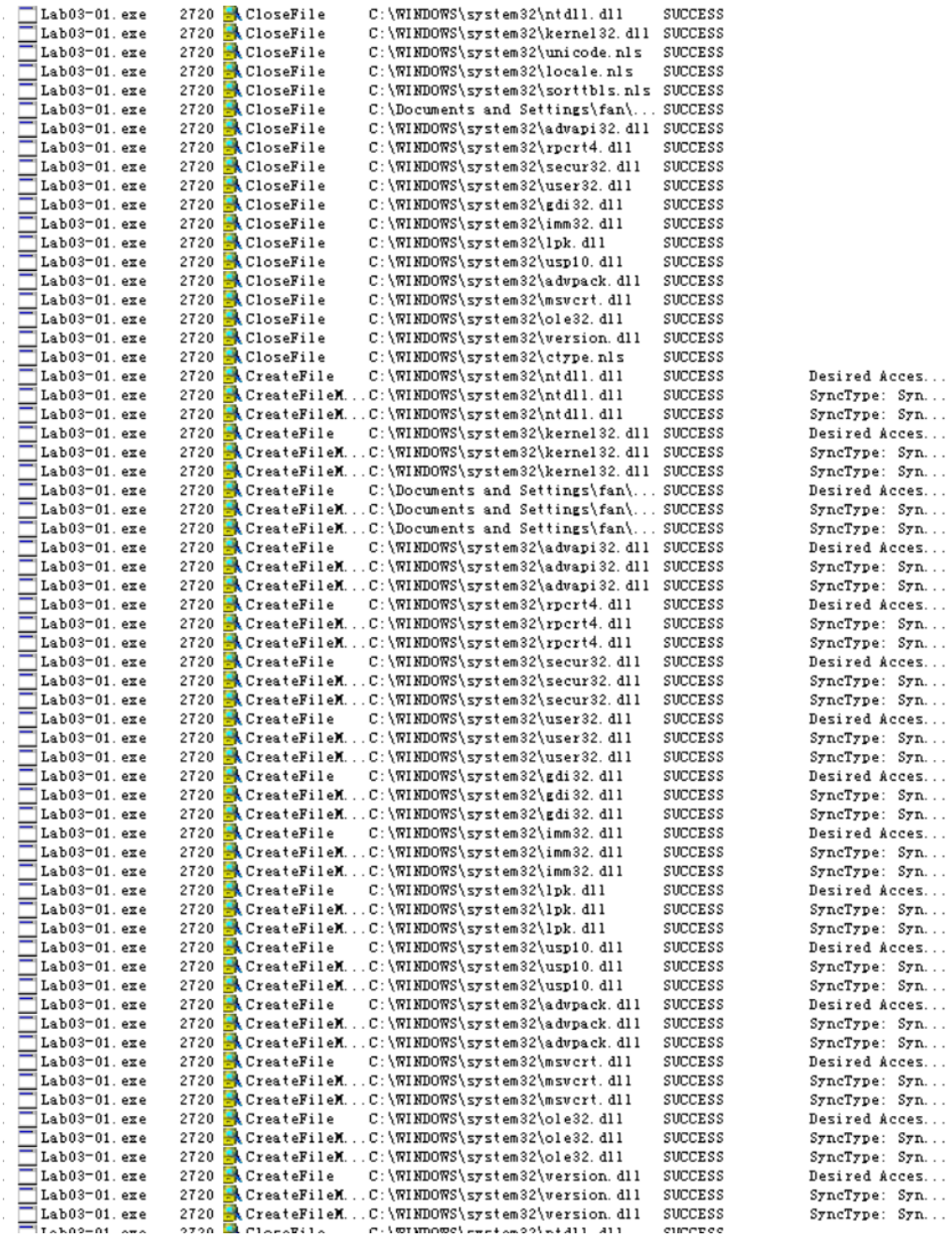
查看 Process Monitor 对进程行为的监视结果，了解该恶意代码都做了哪些方面的事情。

该恶意代码进行了以下内容：遍历了大量目录并对大量的 dll 文件进行了操作；对注册表键值对进行了大量的新建或修改；有网络行为，建立了 TCP 连接。

10:5...	Lab03-01.exe	2720	CloseFile	C:\	SUCCESS	
10:5...	Lab03-01.exe	2720	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	QueryDirectory	C:\Documents and Settings	SUCCESS	0: ., 1: .., ...
10:5...	Lab03-01.exe	2720	QueryDirectory	C:\Documents and Settings	NO MORE FILES	
10:5...	Lab03-01.exe	2720	CloseFile	C:\Documents and Settings	SUCCESS	
10:5...	Lab03-01.exe	2720	CreateFile	C:\Documents and Settings\fan	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	QueryDirectory	C:\Documents and Settings\fan	SUCCESS	0: ., 1: .., ...
10:5...	Lab03-01.exe	2720	QueryDirectory	C:\Documents and Settings\fan	NO MORE FILES	
10:5...	Lab03-01.exe	2720	CloseFile	C:\Documents and Settings\fan	SUCCESS	
10:5...	Lab03-01.exe	2720	CreateFile	C:\Documents and Settings\fan\...	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	QueryDirectory	C:\Documents and Settings\fan\...	SUCCESS	0: ., 1: .., ...
10:5...	Lab03-01.exe	2720	QueryDirectory	C:\Documents and Settings\fan\...	NO MORE FILES	
10:5...	Lab03-01.exe	2720	CloseFile	C:\Documents and Settings\fan\...	SUCCESS	
10:5...	Lab03-01.exe	2720	CreateFile	C:\Documents and Settings\fan\...	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	QueryDirectory	C:\Documents and Settings\fan\...	SUCCESS	0: ., 1: .., ...
10:5...	Lab03-01.exe	2720	QueryDirectory	C:\Documents and Settings\fan\...	NO MORE FILES	
10:5...	Lab03-01.exe	2720	CloseFile	C:\Documents and Settings\fan\...	SUCCESS	
10:5...	Lab03-01.exe	2720	CreateFile	C:\Documents and Settings\fan\...	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	QueryDirectory	C:\Documents and Settings\fan\...	SUCCESS	0: ., 1: .., ...
10:5...	Lab03-01.exe	2720	QueryDirectory	C:\Documents and Settings\fan\...	NO MORE FILES	
10:5...	Lab03-01.exe	2720	CloseFile	C:\Documents and Settings\fan\...	SUCCESS	
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	QueryDirectory	C:\WINDOWS	SUCCESS	0: ., 1: .., ...
10:5...	Lab03-01.exe	2720	QueryDirectory	C:\WINDOWS	NO MORE FILES	
10:5...	Lab03-01.exe	2720	CloseFile	C:\WINDOWS	SUCCESS	
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: ., 1: .., ...
10:5...	Lab03-01.exe	2720	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: dxdiagn.dl...
10:5...	Lab03-01.exe	2720	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: mmcshext.d...
10:5...	Lab03-01.exe	2720	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: racpldlg.d...
10:5...	Lab03-01.exe	2720	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: winhelp.hl...
10:5...	Lab03-01.exe	2720	QueryDirectory	C:\WINDOWS\system32	NO MORE FILES	
10:5...	Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32	SUCCESS	
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\ntdll.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\ntdll.dll	SUCCESS	AllocationSiz...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\ntdll.dll	SUCCESS	SyncType: Syn...

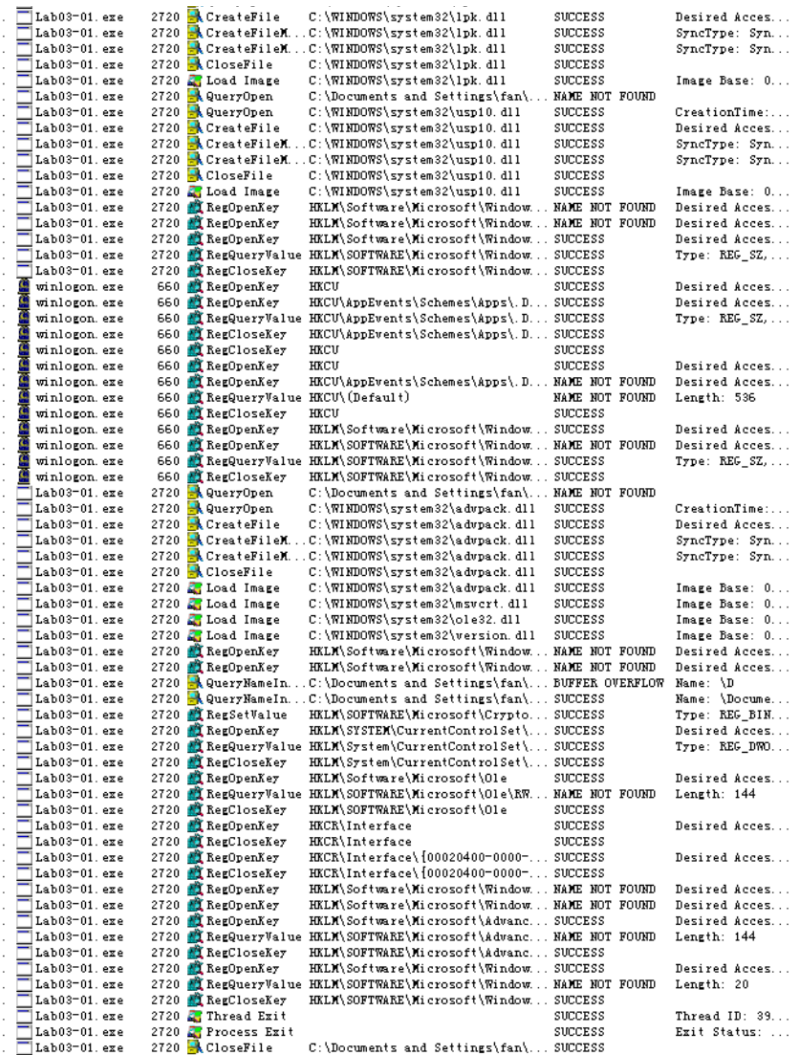
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\kernel32.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\kernel32.dll	SUCCESS	AllocationSiz...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\kernel32.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\unicode.nls	SUCCESS	Desired Acces...
10:5...	Explorer.EXE	1724	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\...	SUCCESS	Desired Acces...
10:5...	Explorer.EXE	1724	RegQueryValue	HKLM\System\CurrentControlSet\...	SUCCESS	Type: REG_DWO...
10:5...	Explorer.EXE	1724	RegQueryValue	HKLM\System\CurrentControlSet\...	SUCCESS	Type: REG_DWO...
10:5...	Explorer.EXE	1724	RegQueryValue	HKLM\System\CurrentControlSet\...	SUCCESS	Type: REG_DWO...
10:5...	Explorer.EXE	1724	RegQueryValue	HKLM\System\CurrentControlSet\...	SUCCESS	Type: REG_SZ, ...
10:5...	Explorer.EXE	1724	RegQueryValue	HKLM\System\CurrentControlSet\...	SUCCESS	Type: REG_SZ, ...
10:5...	Explorer.EXE	1724	RegCloseKey	HKLM\System\CurrentControlSet\...	SUCCESS	
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\unicode.nls	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\unicode.nls	SUCCESS	AllocationSiz...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\unicode.nls	SUCCESS	SyncType: Syn...
10:5...	Explorer.EXE	1724	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\...	SUCCESS	Desired Acces...
10:5...	Explorer.EXE	1724	RegQueryValue	HKLM\System\CurrentControlSet\...	SUCCESS	Type: REG_DWO...
10:5...	Explorer.EXE	1724	RegQueryValue	HKLM\System\CurrentControlSet\...	NAME NOT FOUND	Length: 144
10:5...	Explorer.EXE	1724	RegQueryValue	HKLM\System\CurrentControlSet\...	NAME NOT FOUND	Length: 144
10:5...	Explorer.EXE	1724	RegQueryValue	HKLM\System\CurrentControlSet\...	NAME NOT FOUND	Length: 144
10:5...	Explorer.EXE	1724	RegCloseKey	HKLM\System\CurrentControlSet\...	SUCCESS	
10:5...	Explorer.EXE	1724	RegQueryValue	HKLM\System\CurrentControlSet\...	BUFFER OVERFLOW	Length: 144
10:5...	Explorer.EXE	1724	RegQueryValue	HKLM\System\CurrentControlSet\...	BUFFER OVERFLOW	Length: 144
10:5...	Explorer.EXE	1724	RegQueryValue	HKLM\System\CurrentControlSet\...	SUCCESS	Type: REG_MUL...
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\locale.nls	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\locale.nls	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\locale.nls	SUCCESS	AllocationSiz...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\locale.nls	SUCCESS	SyncType: Syn...
10:5...	Explorer.EXE	1724	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\...	SUCCESS	Desired Acces...
10:5...	Explorer.EXE	1724	RegQueryValue	HKLM\System\CurrentControlSet\...	SUCCESS	Type: REG_DWO...
10:5...	Explorer.EXE	1724	RegQueryValue	HKLM\System\CurrentControlSet\...	SUCCESS	Type: REG_DWO...
10:5...	Explorer.EXE	1724	RegQueryValue	HKLM\System\CurrentControlSet\...	SUCCESS	Type: REG_DWO...
10:5...	Explorer.EXE	1724	RegQueryValue	HKLM\System\CurrentControlSet\...	SUCCESS	Type: REG_SZ, ...
10:5...	Explorer.EXE	1724	RegQueryValue	HKLM\System\CurrentControlSet\...	SUCCESS	Type: REG_SZ, ...
10:5...	Explorer.EXE	1724	RegCloseKey	HKLM\System\CurrentControlSet\...	SUCCESS	
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\sorttbls.nls	SUCCESS	Desired Acces...

10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\sorttbls.nls	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\sorttbls.nls	SUCCESS	AllocationSiz...
10:5...	Explorer.EXE	1724	RegQueryValue	HKLM\System\CurrentControlSet\...	SUCCESS	Type: REG_DWO...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\sorttbls.nls	SUCCESS	SyncType: Syn...
10:5...	Explorer.EXE	1724	RegCloseKey	HKLM\System\CurrentControlSet\...	SUCCESS	
10:5...	Lab03-01.exe	2720	CreateFile	C:\Documents and Settings\fan\...	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\Documents and Settings\fan\...	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\Documents and Settings\fan\...	SUCCESS	AllocationSiz...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\Documents and Settings\fan\...	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\advapi32.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\advapi32.dll	SUCCESS	AllocationSiz...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\advapi32.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	AllocationSiz...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\secur32.dll	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\secur32.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\secur32.dll	SUCCESS	AllocationSiz...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\secur32.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\user32.dll	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\user32.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\user32.dll	SUCCESS	AllocationSiz...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\user32.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\gdi32.dll	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\gdi32.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\gdi32.dll	SUCCESS	AllocationSiz...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\gdi32.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\imm32.dll	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\imm32.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\imm32.dll	SUCCESS	AllocationSiz...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\imm32.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\lpk.dll	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\lpk.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\lpk.dll	SUCCESS	AllocationSiz...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\lpk.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\usp10.dll	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\usp10.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\usp10.dll	SUCCESS	AllocationSiz...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\usp10.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\advpack.dll	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\advpack.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\advpack.dll	SUCCESS	AllocationSiz...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\advpack.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	AllocationSiz...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\ole32.dll	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\ole32.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\ole32.dll	SUCCESS	AllocationSiz...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\ole32.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\version.dll	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\version.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\version.dll	SUCCESS	AllocationSiz...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\version.dll	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\ctype.nls	SUCCESS	Desired Acces...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\ctype.nls	SUCCESS	SyncType: Syn...
10:5...	Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\ctype.nls	SUCCESS	AllocationSiz...
10:5...	Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\ctype.nls	SUCCESS	SyncType: Syn...



Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\unicode.nls	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\locale.nls	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\sorttbls.nls	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\Documents and Settings\fan\...	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\secur32.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\user32.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\gdi32.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\imm32.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\lpk.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\usp10.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\advpack.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\ole32.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\version.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\ctype.nls	SUCCESS	
Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\ntdll.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\ntdll.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\kernel32.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\kernel32.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFile	C:\Documents and Settings\fan\...	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\Documents and Settings\fan\...	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFileM...	C:\Documents and Settings\fan\...	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\advapi32.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\advapi32.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\secur32.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\secur32.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\secur32.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\user32.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\user32.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\user32.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\gdi32.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\gdi32.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\gdi32.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\imm32.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\imm32.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\imm32.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\lpk.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\lpk.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\lpk.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\usp10.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\usp10.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\usp10.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\advpack.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\advpack.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\advpack.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\ole32.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\ole32.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\ole32.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\version.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\version.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\version.dll	SUCCESS	SyncType: Syn...

Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\Documents and Settings\fan\...	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\secur32.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\user32.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\gdi32.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\imm32.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\lpk.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\usp10.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\advpack.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\ole32.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\version.dll	SUCCESS	
Lab03-01.exe	2720	CloseFile	C:	SUCCESS	
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Window...	NAME NOT FOUND	Desired Acces...
Lab03-01.exe	2720	CreateFile	C:\Documents and Settings\fan\...	SUCCESS	Desired Acces...
Lab03-01.exe	2720	FileSystemC...	C:\Documents and Settings\fan\...	SUCCESS	Control: FSCT...
Lab03-01.exe	2720	QueryOpen	C:\Documents and Settings\fan\...	NAME NOT FOUND	
Lab03-01.exe	2720	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0...
Lab03-01.exe	2720	RegOpenKey	HKLM\System\CurrentControlSet\...	SUCCESS	Desired Acces...
Lab03-01.exe	2720	RegQueryValue	HKLM\System\CurrentControlSet\...	SUCCESS	Type: REG_DWO...
Lab03-01.exe	2720	RegCloseKey	HKLM\System\CurrentControlSet\...	SUCCESS	
Lab03-01.exe	2720	RegOpenKey	HKLM\System\CurrentControlSet\...	SUCCESS	Desired Acces...
Lab03-01.exe	2720	RegQueryValue	HKLM\System\CurrentControlSet\...	SUCCESS	Type: REG_DWO...
Lab03-01.exe	2720	RegCloseKey	HKLM\System\CurrentControlSet\...	SUCCESS	
Lab03-01.exe	2720	RegOpenKey	HKLM\System\CurrentControlSet\...	SUCCESS	Desired Acces...
Lab03-01.exe	2720	RegQueryValue	HKLM\System\CurrentControlSet\...	NAME NOT FOUND	Length: 16
Lab03-01.exe	2720	RegCloseKey	HKLM\System\CurrentControlSet\...	SUCCESS	
Lab03-01.exe	2720	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0...
Lab03-01.exe	2720	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0...
Lab03-01.exe	2720	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0...
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Window...	NAME NOT FOUND	Desired Acces...
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Window...	NAME NOT FOUND	Desired Acces...
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Window...	NAME NOT FOUND	Desired Acces...
Lab03-01.exe	2720	RegOpenKey	HKLM\System\CurrentControlSet\...	SUCCESS	Desired Acces...
Lab03-01.exe	2720	RegQueryValue	HKLM\System\CurrentControlSet\...	SUCCESS	Type: REG_DWO...
Lab03-01.exe	2720	RegQueryValue	HKLM\System\CurrentControlSet\...	SUCCESS	Type: REG_DWO...
Lab03-01.exe	2720	RegCloseKey	HKLM\System\CurrentControlSet\...	SUCCESS	
Lab03-01.exe	2720	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Acces...
Lab03-01.exe	2720	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 144
Lab03-01.exe	2720	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
Lab03-01.exe	2720	RegOpenKey	HKLM	SUCCESS	Desired Acces...
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Window...	NAME NOT FOUND	Desired Acces...
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Window...	NAME NOT FOUND	Desired Acces...
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Window...	NAME NOT FOUND	Desired Acces...
Lab03-01.exe	2720	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0...
Lab03-01.exe	2720	Load Image	C:\WINDOWS\system32\gdi32.dll	SUCCESS	Image Base: 0...
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Window...	NAME NOT FOUND	Desired Acces...
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Window...	NAME NOT FOUND	Desired Acces...
Lab03-01.exe	2720	QueryOpen	C:\WINDOWS\system32\imm32.dll	SUCCESS	CreationTime:...
Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\imm32.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\imm32.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\imm32.dll	SUCCESS	AllocationSiz...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\imm32.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\imm32.dll	SUCCESS	
Lab03-01.exe	2720	QueryOpen	C:\WINDOWS\system32\imm32.dll	SUCCESS	CreationTime:...
Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\imm32.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\imm32.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	QueryStanda...	C:\WINDOWS\system32\imm32.dll	SUCCESS	AllocationSiz...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\imm32.dll	SUCCESS	SyncType: Syn...



Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\lpk.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\lpk.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\lpk.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\lpk.dll	SUCCESS	
Lab03-01.exe	2720	Load Image	C:\WINDOWS\system32\lpk.dll	SUCCESS	Image Base: 0...
Lab03-01.exe	2720	QueryOpen	C:\Documents and Settings\fan\...	NAME NOT FOUND	
Lab03-01.exe	2720	QueryOpen	C:\WINDOWS\system32\usp10.dll	SUCCESS	CreationTime:...
Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\usp10.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\usp10.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\usp10.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\usp10.dll	SUCCESS	
Lab03-01.exe	2720	Load Image	C:\WINDOWS\system32\usp10.dll	SUCCESS	Image Base: 0...
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Window...	NAME NOT FOUND	Desired Acces...
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Window...	NAME NOT FOUND	Desired Acces...
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Window...	SUCCESS	Desired Acces...
Lab03-01.exe	2720	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_SZ,...
Lab03-01.exe	2720	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
winlogon.exe	660	RegOpenKey	HKCU	SUCCESS	Desired Acces...
winlogon.exe	660	RegOpenKey	HKCU\AppEvents\Schemes\Apps\.D...	SUCCESS	Desired Acces...
winlogon.exe	660	RegQueryValue	HKCU\AppEvents\Schemes\Apps\.D...	SUCCESS	Type: REG_SZ,...
winlogon.exe	660	RegCloseKey	HKCU\AppEvents\Schemes\Apps\.D...	SUCCESS	
winlogon.exe	660	RegCloseKey	HKCU	SUCCESS	
winlogon.exe	660	RegOpenKey	HKCU	SUCCESS	Desired Acces...
winlogon.exe	660	RegOpenKey	HKCU\AppEvents\Schemes\Apps\.D...	NAME NOT FOUND	Desired Acces...
winlogon.exe	660	RegQueryValue	HKCU\(Default)	NAME NOT FOUND	Length: 536
winlogon.exe	660	RegCloseKey	HKCU	SUCCESS	
winlogon.exe	660	RegOpenKey	HKLM\Software\Microsoft\Window...	SUCCESS	Desired Acces...
winlogon.exe	660	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Desired Acces...
winlogon.exe	660	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_SZ,...
winlogon.exe	660	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
Lab03-01.exe	2720	QueryOpen	C:\Documents and Settings\fan\...	NAME NOT FOUND	
Lab03-01.exe	2720	QueryOpen	C:\WINDOWS\system32\advpack.dll	SUCCESS	CreationTime:...
Lab03-01.exe	2720	CreateFile	C:\WINDOWS\system32\advpack.dll	SUCCESS	Desired Acces...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\advpack.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CreateFileM...	C:\WINDOWS\system32\advpack.dll	SUCCESS	SyncType: Syn...
Lab03-01.exe	2720	CloseFile	C:\WINDOWS\system32\advpack.dll	SUCCESS	
Lab03-01.exe	2720	Load Image	C:\WINDOWS\system32\advpack.dll	SUCCESS	Image Base: 0...
Lab03-01.exe	2720	Load Image	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	Image Base: 0...
Lab03-01.exe	2720	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0...
Lab03-01.exe	2720	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0...
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Window...	NAME NOT FOUND	Desired Acces...
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Window...	NAME NOT FOUND	Desired Acces...
Lab03-01.exe	2720	QueryNameIn...	C:\Documents and Settings\fan\...	BUFFER OVERFLOW	Name: \D
Lab03-01.exe	2720	QueryNameIn...	C:\Documents and Settings\fan\...	SUCCESS	Name: \Docume...
Lab03-01.exe	2720	RegSetValue	HKLM\SOFTWARE\Microsoft\Crypto...	SUCCESS	Type: REG_BIN...
Lab03-01.exe	2720	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\...	SUCCESS	Desired Acces...
Lab03-01.exe	2720	RegQueryValue	HKLM\System\CurrentControlSet\...	SUCCESS	Type: REG_DWO...
Lab03-01.exe	2720	RegCloseKey	HKLM\System\CurrentControlSet\...	SUCCESS	
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Ole	SUCCESS	Desired Acces...
Lab03-01.exe	2720	RegQueryValue	HKLM\SOFTWARE\Microsoft\Ole\RW...	NAME NOT FOUND	Length: 144
Lab03-01.exe	2720	RegCloseKey	HKLM\SOFTWARE\Microsoft\Ole	SUCCESS	
Lab03-01.exe	2720	RegOpenKey	HKCR\Interface	SUCCESS	Desired Acces...
Lab03-01.exe	2720	RegCloseKey	HKCR\Interface	SUCCESS	
Lab03-01.exe	2720	RegOpenKey	HKCR\Interface\{00020400-0000-...	SUCCESS	Desired Acces...
Lab03-01.exe	2720	RegCloseKey	HKCR\Interface\{00020400-0000-...	SUCCESS	
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Window...	NAME NOT FOUND	Desired Acces...
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Window...	NAME NOT FOUND	Desired Acces...
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Advanc...	SUCCESS	Desired Acces...
Lab03-01.exe	2720	RegQueryValue	HKLM\SOFTWARE\Microsoft\Advanc...	NAME NOT FOUND	Length: 144
Lab03-01.exe	2720	RegCloseKey	HKLM\SOFTWARE\Microsoft\Advanc...	SUCCESS	
Lab03-01.exe	2720	RegOpenKey	HKLM\Software\Microsoft\Window...	SUCCESS	Desired Acces...
Lab03-01.exe	2720	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 20
Lab03-01.exe	2720	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
Lab03-01.exe	2720	Thread Exit		SUCCESS	Thread ID: 39...
Lab03-01.exe	2720	Process Exit		SUCCESS	Exit Status: ...
Lab03-01.exe	2720	CloseFile	C:\Documents and Settings\fan\...	SUCCESS	

ApateDNS 监测到恶意代码向域名 www.practicalmalwareanalysis.com 发送了请求。并且该请求每隔 61 秒重新发送一次。

在 Regshot 上点击“建立快照 B”，拍摄第二份快照并保存报告，然后点击“比较快照”。

快照比较内容如下：

```
Regshot 1.8.3-beta1U5
Comments:
Datetime:2024/10/9 02:46:10  ,  2024/10/9 03:03:26
Computer:WINXP , WINXP
Username:fan , fan

----------------------------------
Keys added:6
----------------------------------
HKU\S-1-5-21-507921405-128422742-1801674531-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\hiv
HKU\S-1-5-21-507921405-128422742-1801674531-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hiv
HKU\S-1-5-21-507921405-128422742-1801674531-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hiv\OpenWithList
HKU\S-1-5-21-507921405-128422742-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\BagMRU\7
HKU\S-1-5-21-507921405-128422742-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62
HKU\S-1-5-21-507921405-128422742-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell

----------------------------------
Values deleted:2
----------------------------------
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\0: "SW\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"
HKLM\SYSTEM\CurrentControlSet\Services\kmixer\Enum\0: "SW\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"
```

```
----------------------------------
Values added:38
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver: 43 3A 5C 57 49 4E 44 4F 57 53 5C 73 79 73 74 65 6D 33 32 5C 76 6D 78 33 32 74 6F 36 34 2
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU\b: 72 00 65 00 67 00 73 00
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*\b: "C:\Documents and Setting
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\hiv\a: "C:\Documents and Setti
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\hiv\MRUList: "a"
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hiv\OpenWithList\a: "regshot.exe"
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hiv\OpenWithList\MRUList: "a"
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\C
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\BagMRU\7: 34 00 31 00 00 00 00 00 49 59 8C 15 10 00 6C 61 62 33
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\BagMRU\7\NodeSlot: 0x0000003E
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\BagMRU\7\MRUListEx: FF FF FF FF
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\MinPos1240x1005(1).x: 0xFFFFFFFF
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\MinPos1240x1005(1).y: 0xFFFFFFFF
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\MaxPos1240x1005(1).x: 0xFFFFFFFF
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\MaxPos1240x1005(1).y: 0xFFFFFFFF
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\WinPos1240x1005(1).left: 0x00000016
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\WinPos1240x1005(1).top: 0x0000001D
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\WinPos1240x1005(1).right: 0x00000336
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\WinPos1240x1005(1).bottom: 0x00000275
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\Rev: 0x00000000
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\WFlags: 0x00000000
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\ShowCmd: 0x00000001
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\FFlags: 0x00000001
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\HotKey: 0x00000000
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\Buttons: 0xFFFFFFFF
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\Links: 0x00000000
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\Address: 0x00000000
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\Vid: "{65F125E5-7BE1-4810-BA9D-D271C8432CE3}"
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\Mode: 0x00000006
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\ScrollPos1240x1005(1).x: 0x00000000
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\ScrollPos1240x1005(1).y: 0x00000000
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\Sort: 0x00000000
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\SortDir: 0x00000001
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\Col: 0xFFFFFFFF
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\ColInfo: 00 00 00 00 00 00 00 00 00 00 00 00 00 0
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\SHELL32.dll,-22913: "显示连接到此
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\SHELL32.dll,-22912: "显示到网站,
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Documents and Settings\fan\桌面\上机实验样本\Chapte
```

```
----------------------------------
Values modified:36
----------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 97 75 36 5F B3 B5 AB 66 D3 7B 74 CC 4C 7B 41 CE 7D 27 E5 EA 5F 40 D1 93 BE 59 BE D4 E3 11 58 23 C5 D5 24
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: CB 59 93 04 AF 5D 66 6B DE D1 14 49 B6 76 B0 7C 57 2C 6E 4C 99 5B 3C 1A 16 25 09 13 39 39 E2 C3 81 06 34
HKLM\SYSTEM\ControlSet001\Services\Dhcp\Parameters\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}: 2C 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 A3 F3 05 67 C
HKLM\SYSTEM\ControlSet001\Services\Dhcp\Parameters\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}: 2C 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 27 F7 05 67 C
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\Count: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\Count: 0x00000000
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\NextInstance: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\NextInstance: 0x00000000
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Epoch\Epoch: 0x00000027
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Epoch\Epoch: 0x00000029
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\LeaseObtainedTime: 0x6705EC9B
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\LeaseObtainedTime: 0x6705F01F
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\T1: 0x6705F01F
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\T1: 0x6705F3A3
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\T2: 0x6705F2C2
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\T2: 0x6705F646
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\LeaseTerminatesTime: 0x6705F3A3
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\LeaseTerminatesTime: 0x6705F727
HKLM\SYSTEM\ControlSet001\Services\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\Parameters\Tcpip\LeaseObtainedTime: 0x6705EC9B
HKLM\SYSTEM\ControlSet001\Services\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\Parameters\Tcpip\LeaseObtainedTime: 0x6705F01F
HKLM\SYSTEM\ControlSet001\Services\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\Parameters\Tcpip\T1: 0x6705F01F
HKLM\SYSTEM\ControlSet001\Services\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\Parameters\Tcpip\T1: 0x6705F3A3
HKLM\SYSTEM\ControlSet001\Services\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\Parameters\Tcpip\T2: 0x6705F2C2
HKLM\SYSTEM\ControlSet001\Services\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\Parameters\Tcpip\T2: 0x6705F646
HKLM\SYSTEM\ControlSet001\Services\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\Parameters\Tcpip\LeaseTerminatesTime: 0x6705F3A3
HKLM\SYSTEM\ControlSet001\Services\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\Parameters\Tcpip\LeaseTerminatesTime: 0x6705F727
HKLM\SYSTEM\CurrentControlSet\Services\Dhcp\Parameters\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}: 2C 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 A3 F3 05
HKLM\SYSTEM\CurrentControlSet\Services\Dhcp\Parameters\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}: 2C 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 27 F7 05
HKLM\SYSTEM\CurrentControlSet\Services\kmixer\Enum\Count: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\kmixer\Enum\Count: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Services\kmixer\Enum\NextInstance: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\kmixer\Enum\NextInstance: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Epoch\Epoch: 0x00000027
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Epoch\Epoch: 0x00000029
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\LeaseObtainedTime: 0x6705EC9B
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\LeaseObtainedTime: 0x6705F01F
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\T1: 0x6705F01F
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\T1: 0x6705F3A3
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\T2: 0x6705F2C2
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\T2: 0x6705F646
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\LeaseTerminatesTime: 0x6705F3A3
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\LeaseTerminatesTime: 0x6705F727
HKLM\SYSTEM\CurrentControlSet\Services\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\Parameters\Tcpip\LeaseObtainedTime: 0x6705EC9B
HKLM\SYSTEM\CurrentControlSet\Services\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\Parameters\Tcpip\LeaseObtainedTime: 0x6705F01F
HKLM\SYSTEM\CurrentControlSet\Services\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\Parameters\Tcpip\T1: 0x6705F01F
HKLM\SYSTEM\CurrentControlSet\Services\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\Parameters\Tcpip\T1: 0x6705F3A3
HKLM\SYSTEM\CurrentControlSet\Services\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\Parameters\Tcpip\T2: 0x6705F2C2
HKLM\SYSTEM\CurrentControlSet\Services\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\Parameters\Tcpip\T2: 0x6705F646
```

```
HKLM\SYSTEM\CurrentControlSet\Services\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\Parameters\Tcpip\LeaseTerminatesTime: 0x6705F3A3
HKLM\SYSTEM\CurrentControlSet\Services\{1EAB93DE-53F2-42E1-8F74-16C2D838B22C}\Parameters\Tcpip\LeaseTerminatesTime: 0x6705F727
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU\MRUList: "a"
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU\MRUList: "ba"
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*\MRUList: "a"
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\*\MRUList: "ba"
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\C
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\C
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\C
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\C
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\BagMRU\NodeSlots: 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\BagMRU\NodeSlots: 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx: 01 00 00 00 02 00 00 00 06 00 00 00 03 00 00
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx: 06 00 00 00 07 00 00 00 03 00 00 00 01 00 00
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\52\Shell\WinPos1240x1005(1).left: 0x0000006E
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\52\Shell\WinPos1240x1005(1).left: 0x0000008B
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\52\Shell\WinPos1240x1005(1).top: 0x00000091
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\52\Shell\WinPos1240x1005(1).top: 0x000000AE
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\52\Shell\WinPos1240x1005(1).right: 0x0000038E
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\52\Shell\WinPos1240x1005(1).right: 0x000003AB
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\52\Shell\WinPos1240x1005(1).bottom: 0x000002E9
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\Software\Microsoft\Windows\ShellNoRoam\Bags\52\Shell\WinPos1240x1005(1).bottom: 0x00000306
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\SessionInformation\ProgramCount: 0x00000007
HKU\S-1-5-21-507921405-1284227242-1801674531-1004\SessionInformation\ProgramCount: 0x00000006

----------------------------------
Total changes:82
----------------------------------
```

3. 这个恶意代码是否存在一些有用的网络特征码?如果存在,它们是什么?

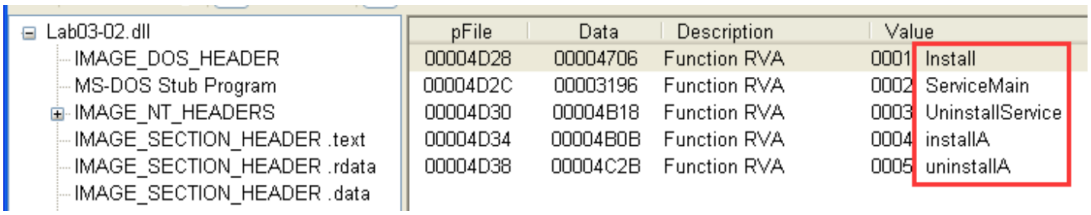
该恶意代码虽然有访问网站的行为，但没有其他下载、请求资源或页面的行为，网络特征码应只是网址“*www.practicalmalwareanalysis.com*”。

• Lab 3-2

使用动态分析基础技术来分析在 Lab03-02.dll 文件中发现的恶意意代码。

1. 你怎样才能让这个恶意代码自行安装?

使用 PEview 查看导出函数。



用于安装的函数为 Install 和 installA，使用 Windows 自带的 rundll32.exe 来调用 installA 函数实现安装，执行命令 rundll32.exe Lab03-02.dll,installA 可以实现这个恶意代码的自行安装。

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

C:\Documents and Settings\fan\桌面\上机实验样本\Chapter_3L>
```

2. 在安装之后,你如何让这个恶意代码运行起来?

执行了安装函数后，并不会返回什么信息，Lab03-02.dll 也并不会因此就变成了 Lab03-02.exe 供我们运行。

用 Regshot 来查看安装前后的注册表变化，观察经过 regshot 对比后的数据，可以观察到一项关于恶意代码的发现。在 key adds 中发现增加了一个 IPRIP 的服务，说明 Lab03-02.dll 将自己安装成一个 IPRIP 服务，说明 dll 需要一个可执行程序来执行它，该恶意代码执行时显示的名字为“Intranet Network Awareness（NIA+），恶意代码的 DLL 文件已被成功挂载在"svchost.exe"进程上运行。

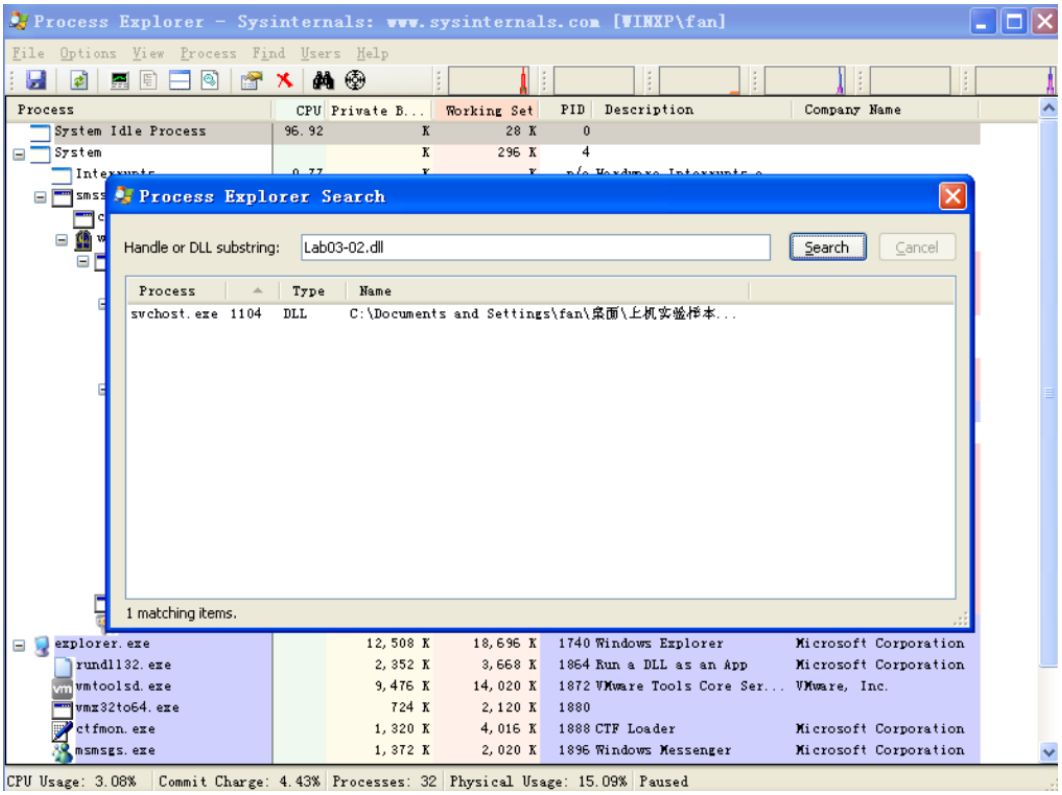
```
HKLM\SOFTWARE\Classes\ocxfile\shell\View Dependencies\command
HKLM\SOFTWARE\Classes\ocxfile\shell\View Dependencies\ddeexec
HKLM\SOFTWARE\Classes\scrfile\shell\View Dependencies
HKLM\SOFTWARE\Classes\scrfile\shell\View Dependencies\command
HKLM\SOFTWARE\Classes\scrfile\shell\View Dependencies\ddeexec
HKLM\SOFTWARE\Classes\sysfile\shell
HKLM\SOFTWARE\Classes\sysfile\shell\View Dependencies
HKLM\SOFTWARE\Classes\sysfile\shell\View Dependencies\command
HKLM\SOFTWARE\Classes\sysfile\shell\View Dependencies\ddeexec
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
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Dependency Walker\Recent File List
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\2\0\3
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\2\0\3\0
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\2\0\3\0\0
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\2\0\3\0\0\0
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\5\14
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\5\14\0
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Windows\ShellNoRoam\Bags\64
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Windows\ShellNoRoam\Bags\64\Shell
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Windows\ShellNoRoam\Bags\65
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Windows\ShellNoRoam\Bags\65\Shell
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Windows\ShellNoRoam\Bags\66
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Windows\ShellNoRoam\Bags\66\Shell
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Windows\ShellNoRoam\Bags\67
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Windows\ShellNoRoam\Bags\67\Shell
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Windows\ShellNoRoam\Bags\68
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Windows\ShellNoRoam\Bags\68\Shell
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Windows\ShellNoRoam\Bags\69
HKU\S-1-5-21-606747145-484763869-1177238915-500\Software\Microsoft\Windows\ShellNoRoam\Bags\69\Shell
```

为执行恶意代码,攻击者可借助'net"命令执行"net start IPRIP"指令,以激活已经部署的恶意代码所依赖的服务。

```
C:\Documents and Settings\fan\桌面\上机实验样本\Chapter_3L>net start IPRIP
Intranet Network Awareness (INA+) 服务正在启动 .
Intranet Network Awareness (INA+) 服务已经启动成功。
```

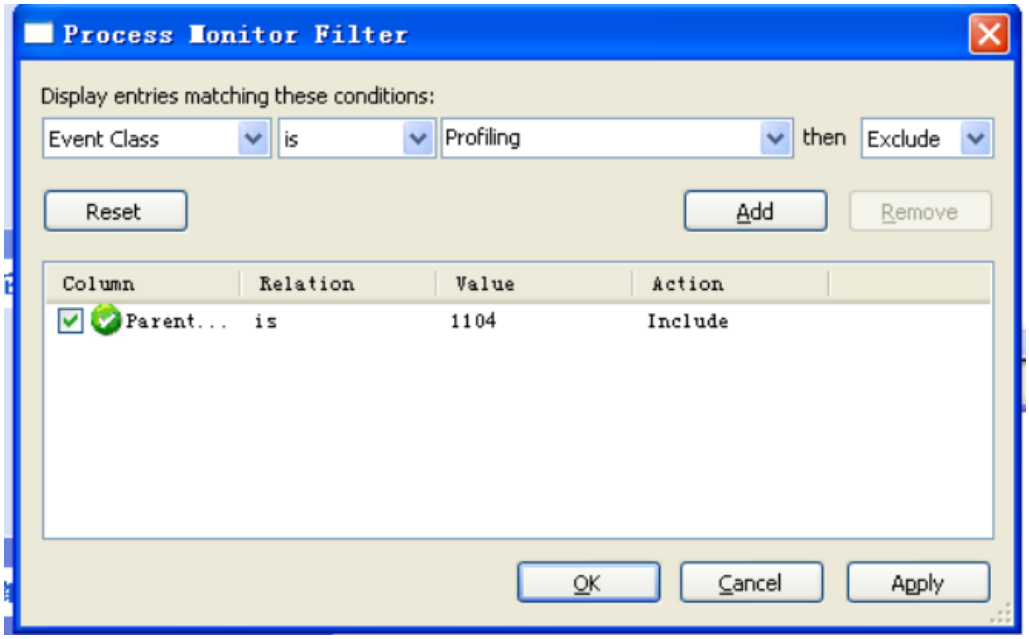
3. 你怎么能找到这个恶意代码是在哪个进程下运行的?

打开 Process Explorer，点击“Find”-“Find Handle or DLL…”，查找“Lab03-02.dll”，发现是在 svchost.exe 进程下运行的。



4. 你可以在 procmon 工具中设置什么样的过滤器,才能收集这个恶意代码的信息?

在 Process Explorer 中可以看出父进程 svchost.exePID 为 1060，过滤器设置如下：

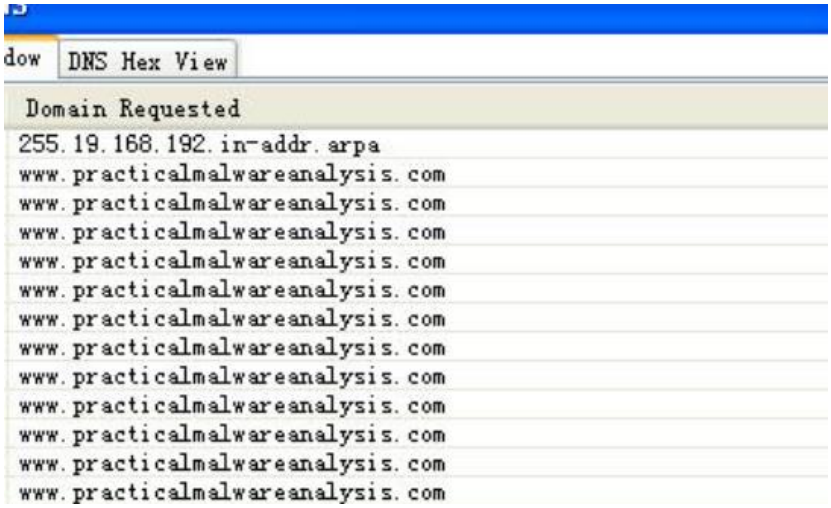


5.这个恶意代码在主机上的感染迹象特征是什么?

相关目录下出现“IPRIP”键；新增了一个 IPRIP 服务，且该服务被设置为开机自动启动。

6.这个恶意代码是否存在一些有用的网络特征码?

分析 ApateDNS，启动 IPRIP 服务后发现 Lab03-02.dll 访问了 practicalmalwareanalysis.com 网址，该网址即是这个恶意代码的网络特征码。



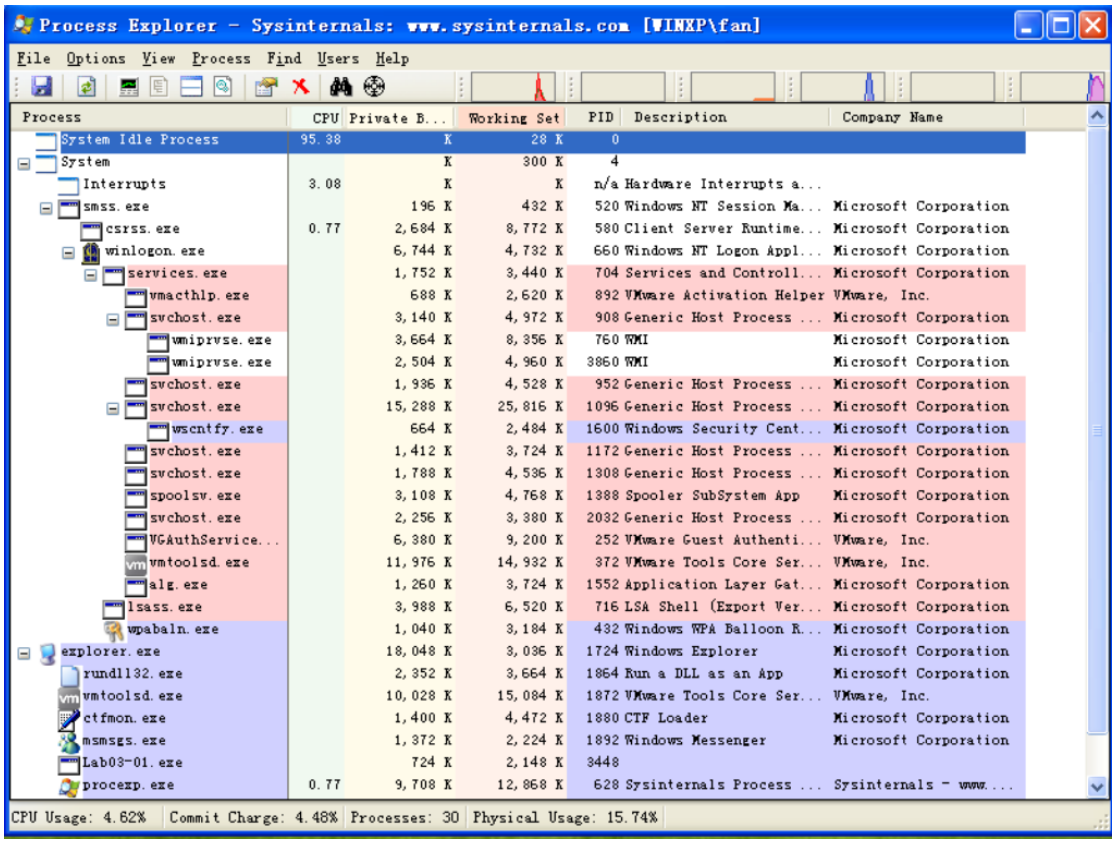
• Lab 3-3

在一个安全的环境中执行 Lab03-03.exe 文件中发现的恶意代码，同时使用基础的动态行为分析工具监视它的行为。

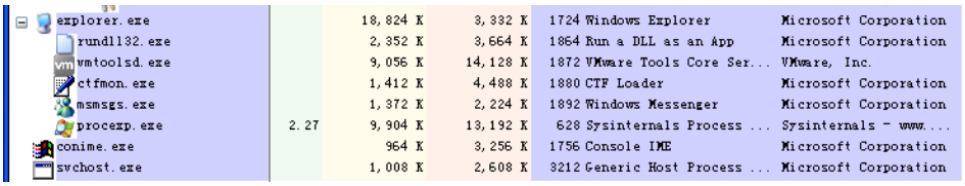
1. 当你使用 Process Explorer 工具进行监视时，你注意到了什么？

先使用 PEiD 查壳，发现 Lab03-03.exe 文件没有加壳。

打开 Process Explorer ，记录下未运行前的进程情况。

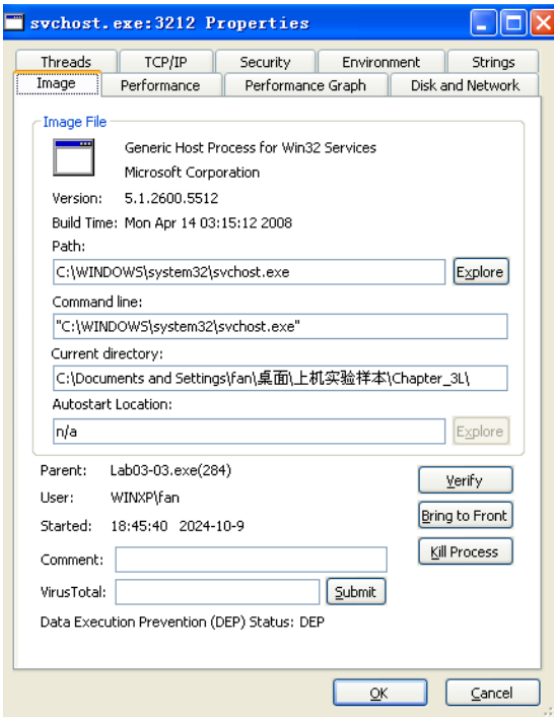


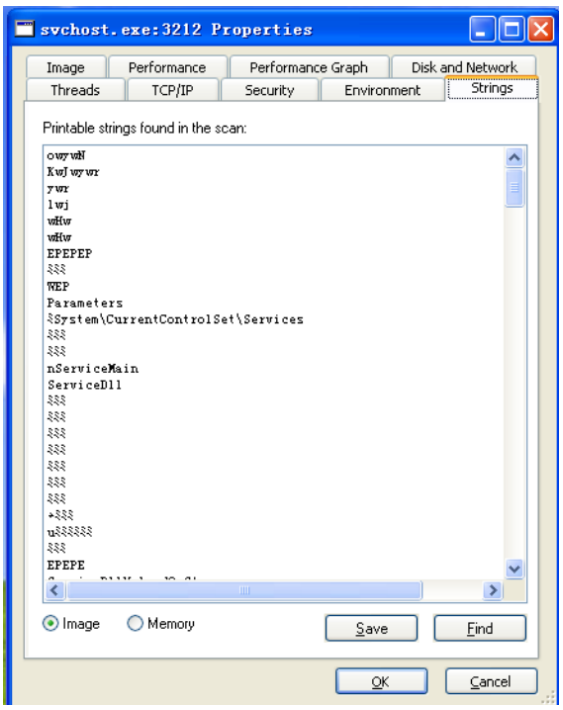
运行 Lab03-03.exe，再次查看 Process Explorer。

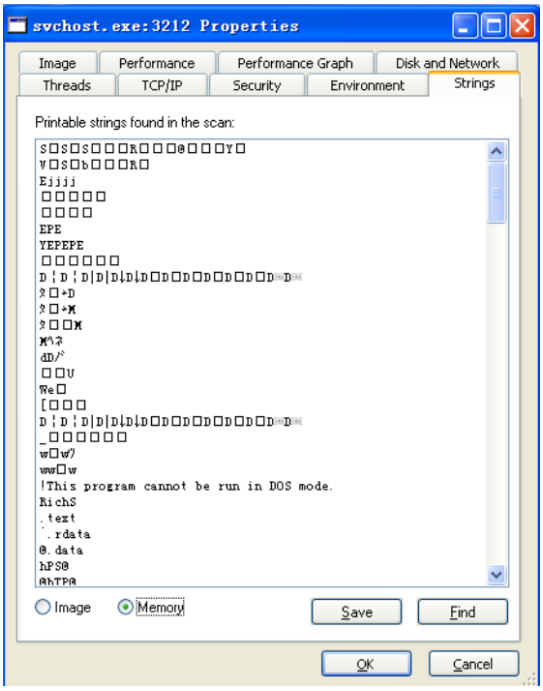


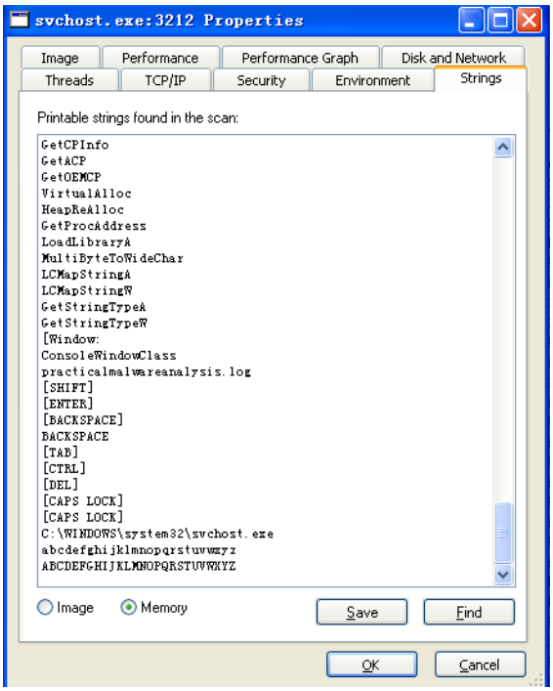
explorer.exe		18,824 K	3,332 K	1724 Windows Explorer	Microsoft Corporation
rundll32.exe		2,352 K	3,664 K	1864 Run a DLL as an App	Microsoft Corporation
vmtoolsd.exe		9,056 K	14,128 K	1872 VMware Tools Core Ser...	VMware, Inc.
ctfmon.exe		1,412 K	4,488 K	1880 CTF Loader	Microsoft Corporation
msmsgs.exe		1,372 K	2,224 K	1892 Windows Messenger	Microsoft Corporation
procexp.exe	2.27	9,904 K	13,192 K	628 Sysinternals Process ...	Sysinternals - www....
conime.exe		964 K	3,256 K	1756 Console IME	Microsoft Corporation
svchost.exe		1,008 K	2,608 K	3212 Generic Host Process ...	Microsoft Corporation

多出来一个“svchost.exe”， 查看“Strings”，分别查看“Image”、“Memory”下的内容。





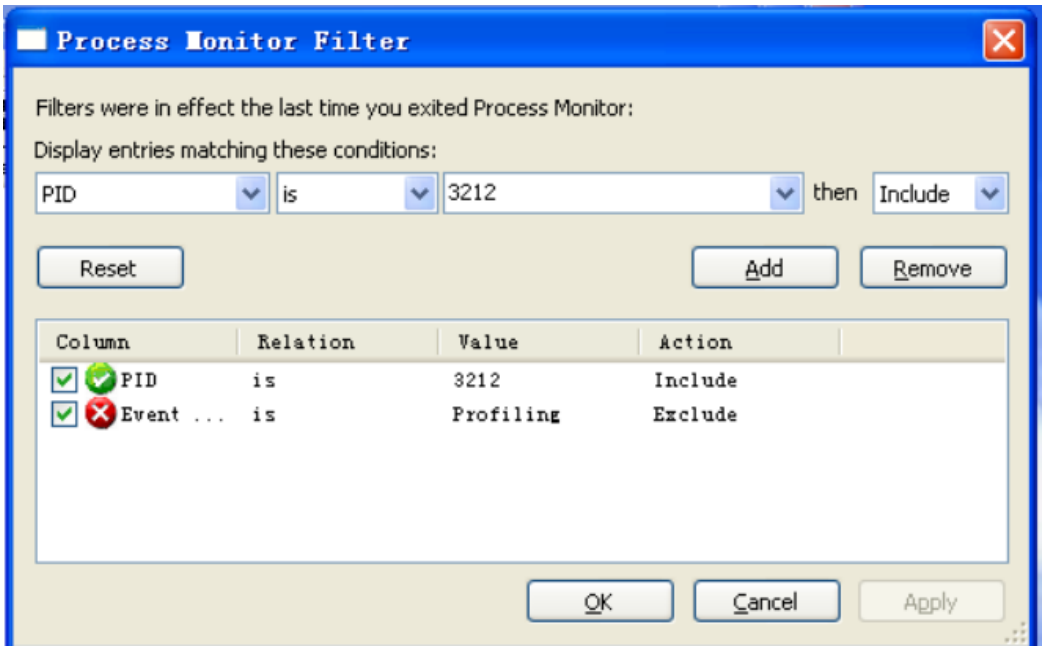


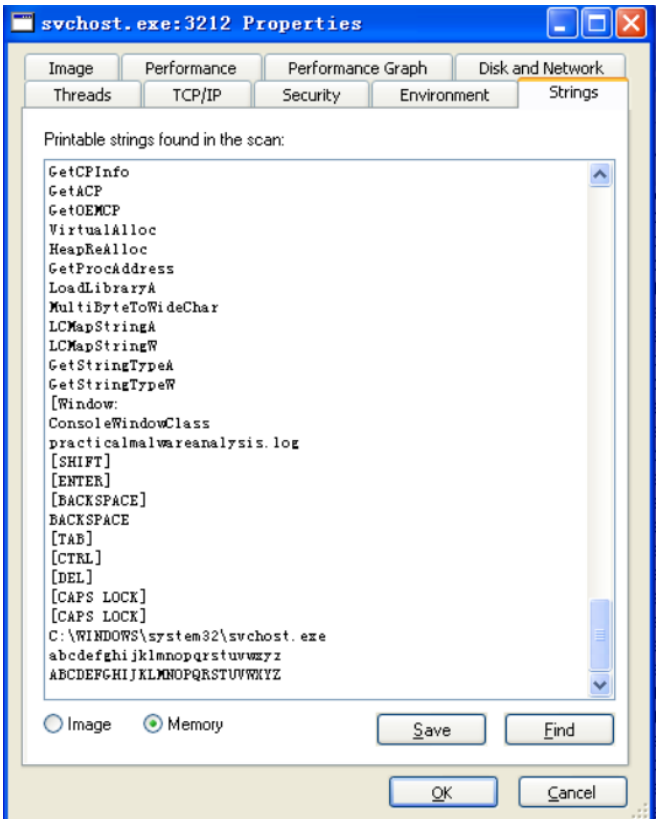


可以确定这是恶意代码运行后创建的进程。恶意代码执行了 svchost.exe 文件的替换。

2. 你可以找出任何的内存修改行为吗?

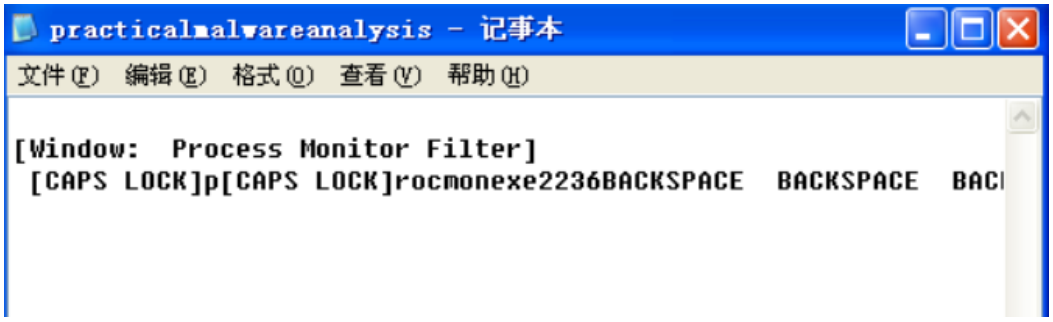
在 Process Explorer 中我们看到 svchost.exe 的 PID 为 3212，因此在 Process Monitor 中过滤，添加 PID is 3212 规则。





对比磁盘和内存中的字符串，发现磁盘镜像和内存镜像中可执行文件的字符串列表差异很大。内存中的字符串多出了 practicalmalwareanalysis.log 和 [SHIFT]、[ENTER]、[BACKSPACE]这样的字符串，而这些通常在正常的 svchost.exe 的磁盘镜像中不应当出现，推测是一个击键的记录器。

3. 这个恶意代码在主机上的感染迹象特征是什么?



有一个“svchost.exe”在运行，且该进程并非 Windows 的系统进程，查看其字符串能看到前一问图中相关内容；计算机中将出现“practicalmalwareanalysis.log”日志文件。

4. 这个恶意代码的目的是什么?

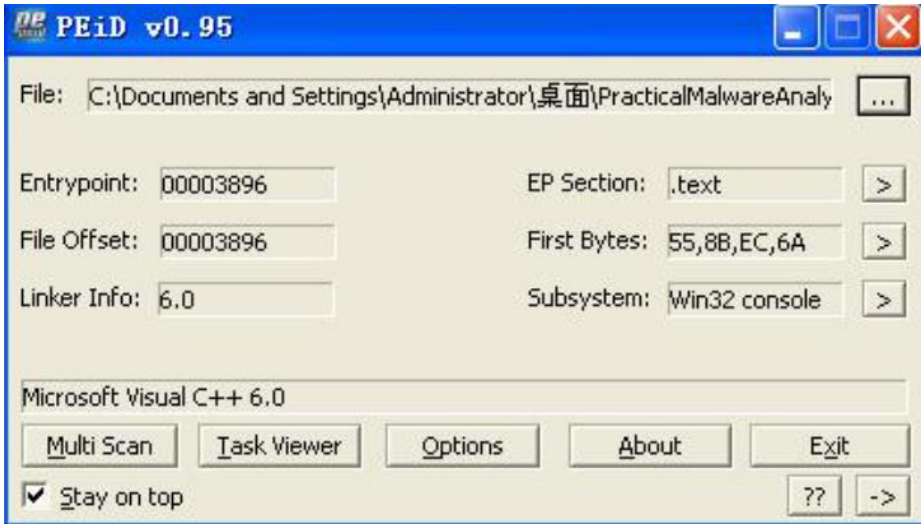
记录用户的键盘输入内容以及在哪里进行的输入，并保存在“practicalmalwareanalysis.log”日志文件中。

• Lab 3-4

使用基础的动态行为分析工具来分析在 Lab03-04.exe 文件中发现的恶意代码。(这个程序还会在第 9 章的实验作业中进一步分析)

1. 当你运行这个文件时,会发生什么呢?

利用 PEID 检查是否存在加壳，可以明显的发现，该应用程序并不存在加壳的现象，因此可以直接分析字符串。

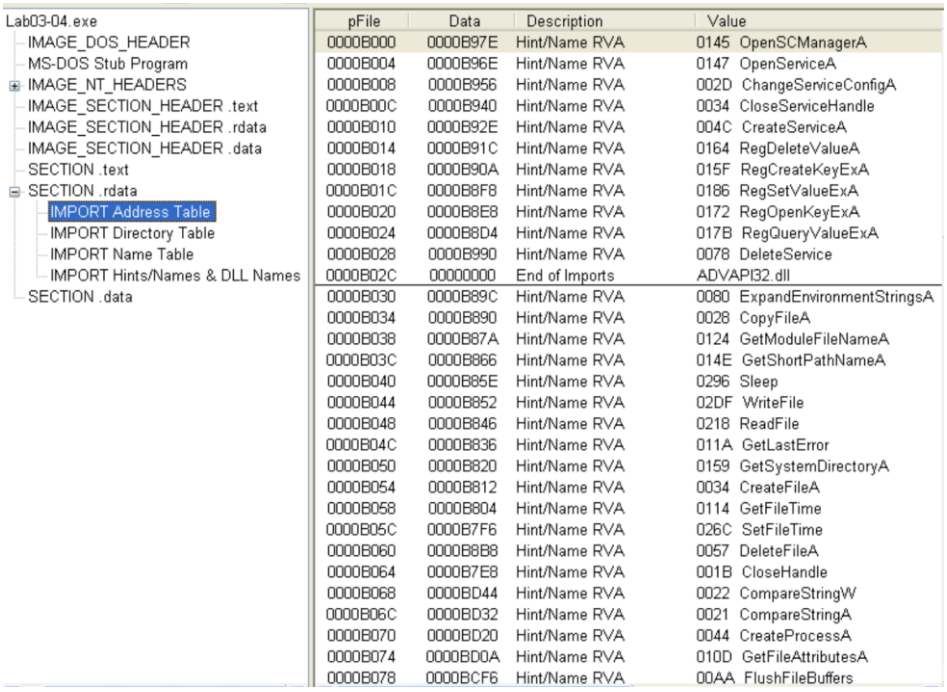


使用 PEview 查看文件，visual size 与 raw data 的大小并不是相同的。

Advapi32.dll 中导入的函数主要与服务和注册表有关，怀疑它可能创建了一个新的服务并运行了，此外之前从 Process Monitor 中也可能看到对注册表进行了大量操作，但是 Regshot 却只发现了一点小修改，怀疑恶意代码运行完后还会恢复注册表的内容防止对其进行动态分析；

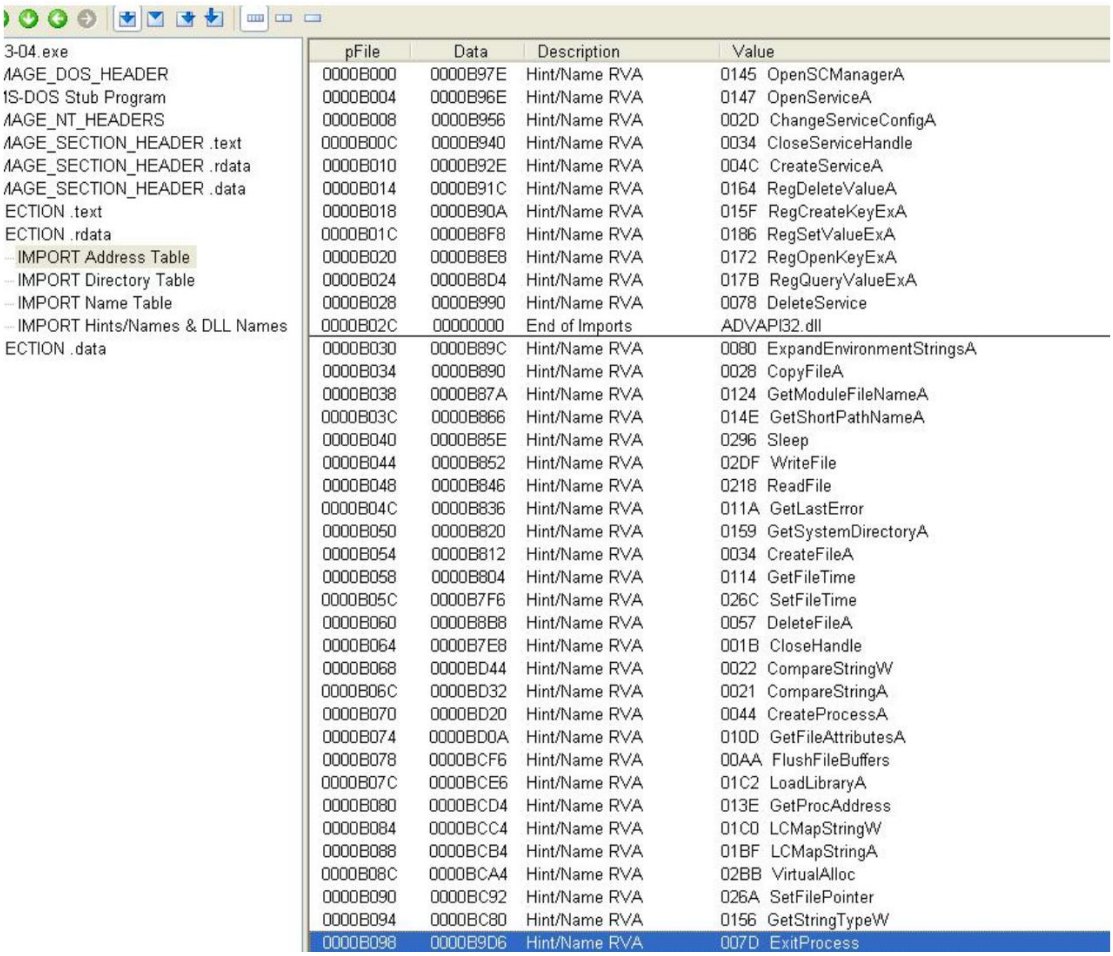
Kernel32.dll 中导入的函数有：文件相关（创建、读、写、删除、复制文件等）、字符串相关（比较字符串、中繁体切换等）、线程同步相关、cmd 相关（打开终端、获取 cmd 中运行该 exe 文件时的参数等）、堆相关等；

Shell32.dll 中导入了 ShellExecuteA 函数，用来执行 cmd 命令；WS2_32.dll 是 Windows Sockets 应用程序接口，用于支持 Internet 和网络应用程序，说明该恶意代码有联网、访问网站行为。



pFile	Data	Description	Value
0000B000	0000B97E	Hint/Name RVA	0145 OpenSCManagerA
0000B004	0000B96E	Hint/Name RVA	0147 OpenServiceA
0000B008	0000B956	Hint/Name RVA	002D ChangeServiceConfigA
0000B00C	0000B940	Hint/Name RVA	0034 CloseServiceHandle
0000B010	0000B92E	Hint/Name RVA	004C CreateServiceA
0000B014	0000B91C	Hint/Name RVA	0164 RegDeleteValueA
0000B018	0000B90A	Hint/Name RVA	015F RegCreateKeyExA
0000B01C	0000B8F8	Hint/Name RVA	0186 RegSetValueExA
0000B020	0000B8E8	Hint/Name RVA	0172 RegOpenKeyExA
0000B024	0000B8D4	Hint/Name RVA	017B RegQueryValueExA
0000B028	0000B990	Hint/Name RVA	0078 DeleteService
0000B02C	00000000	End of Imports	ADVAPI32.dll
0000B030	0000B89C	Hint/Name RVA	0080 ExpandEnvironmentStringsA
0000B034	0000B890	Hint/Name RVA	0028 CopyFileA
0000B038	0000B87A	Hint/Name RVA	0124 GetModuleFileNameA
0000B03C	0000B866	Hint/Name RVA	014E GetShortPathNameA
0000B040	0000B85E	Hint/Name RVA	0296 Sleep
0000B044	0000B852	Hint/Name RVA	02DF WriteFile
0000B048	0000B846	Hint/Name RVA	0218 ReadFile
0000B04C	0000B836	Hint/Name RVA	011A GetLastError
0000B050	0000B820	Hint/Name RVA	0159 GetSystemDirectoryA
0000B054	0000B812	Hint/Name RVA	0034 CreateFileA
0000B058	0000B804	Hint/Name RVA	0114 GetFileTime
0000B05C	0000B7F6	Hint/Name RVA	026C SetFileTime
0000B060	0000B8B8	Hint/Name RVA	0057 DeleteFileA
0000B064	0000B7E8	Hint/Name RVA	001B CloseHandle
0000B068	0000BD44	Hint/Name RVA	0022 CompareStringW
0000B06C	0000BD32	Hint/Name RVA	0021 CompareStringA
0000B070	0000BD20	Hint/Name RVA	0044 CreateProcessA
0000B074	0000BD0A	Hint/Name RVA	010D GetFileAttributesA
0000B078	0000BCF6	Hint/Name RVA	00AA FlushFileBuffers

0000B104	0000BBBE	Hint/Name RVA	0108 GetEnvironmentStringsW
0000B108	0000BBD8	Hint/Name RVA	0126 GetModuleHandleA
0000B10C	0000BBEC	Hint/Name RVA	0109 GetEnvironmentVariableA
0000B110	0000BC06	Hint/Name RVA	0175 GetVersionExA
0000B114	0000BC16	Hint/Name RVA	019D HeapDestroy
0000B118	0000BC24	Hint/Name RVA	019B HeapCreate
0000B11C	0000BC32	Hint/Name RVA	02BF VirtualFree
0000B120	0000BC40	Hint/Name RVA	019F HeapFree
0000B124	0000BC4C	Hint/Name RVA	022F RtlUnwind
0000B128	0000BC58	Hint/Name RVA	01E4 MultiByteToWideChar
0000B12C	0000BC6E	Hint/Name RVA	0153 GetStringTypeA
0000B130	0000BD56	Hint/Name RVA	0262 SetEnvironmentVariableA
0000B134	00000000	End of Imports	KERNEL32.dll
0000B138	0000B9AE	Hint/Name RVA	0072 ShellExecuteA
0000B13C	00000000	End of Imports	SHELL32.dll
0000B140	80000016	Ordinal	0016
0000B144	80000073	Ordinal	0073
0000B148	80000034	Ordinal	0034
0000B14C	80000013	Ordinal	0013
0000B150	80000017	Ordinal	0017
0000B154	80000009	Ordinal	0009
0000B158	80000004	Ordinal	0004
0000B15C	80000003	Ordinal	0003
0000B160	80000010	Ordinal	0010
0000B164	80000074	Ordinal	0074
0000B168	00000000	End of Imports	WS2_32.dll



通过 Strings 查看 Lab03-04.exe 字符串，可以明确看出该恶意代码会有网络访问行为，目标网站是“http://www.practicalmalwareanalysis.com”，且可能会有文件上传、下载行为；该恶意代码也确实会开启终端，并执行了文件删除命令。

根据下图猜测

文件和环境的函数：GetFileAttributes 、GetEnvironmentStrings

系统命令：cmd.exe、/c del、CMD、SLEEP、DOWNLOAD、UPLOAD

疑似命令行参数：-cc、-re、-in、k:%s h:%s p:%s per:%s

HTTP 命令：HTTP/1.0、GET 域 名 ： http://www.practicalmalwareanalysis.com

系统文件：%SYSTEMROOT%\system32\

2. 是什么原因造成动态分析无法有效实施?

尝试运行该应用程序，会发现该程序闪一下之后就会将自身自动删除；有可能需要提供一个命令行参数，或者是这个程序缺失某个部件。

3. 是否有其他方式来运行这个程序?

尝试使用在字符串列表中显示的一些命令行参数 ，比如-cc、-re、-in，但我尝试发现并没有效果。

四、实验结论及心得体会

通过本次实验，我深入了解了恶意软件的分析技术及其复杂性。

静态与动态分析的结合让我意识到仅依靠单一方法难以全面揭示恶意软件的特性。尤其是在监控其动态行为时，使用各种工具（如 Process Explorer 和 ProcessMonitor）显著提高了我对其文件操作和网络活动的理解。

此外，发现恶意软件的持久性机制以及自毁特性，使我认识到分析过程中的挑战性与重要性。整个实验不仅提升了我的技术能力，也增强了我对网络安全威胁的敏感性。