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　2112060

姓　　名　孙蕗

班　　级　信息安全 1 班

《恶意代码分析与防治技术》课程 Lab3 实验报告

一、 实验目的

使用动态分析基础技术来分析恶意代码，包括查找恶意代码的导入函数和字符串列表，监视恶意代码的行为，识别感染迹象特征，以及尝试运行和分析恶意代码的行为。

二、 实验原理

使用各种工具和技术，包括 PEview、strings、Process Explorer、Procmon、Wireshark 等，用于动态分析恶意代码的行为和特征。

通过监视进程、文件、注册表等的变化，可以识别恶意代码的行为和感染迹象。

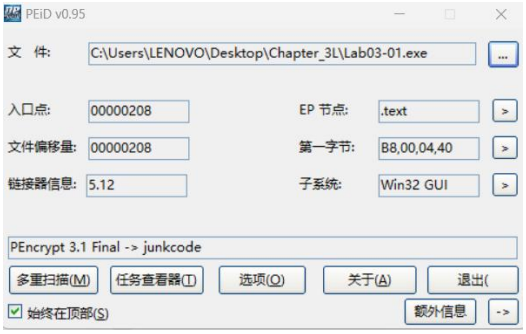
三、 实验过程

（一） Lab3-1

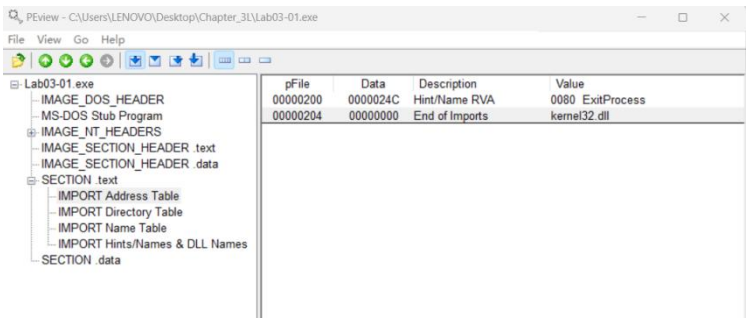
使用动态分析基础技术来分析在 Lab03-01.exe 文件中发现的恶意代码。

（1） 找出这个恶意代码的导入函数与字符串列表。

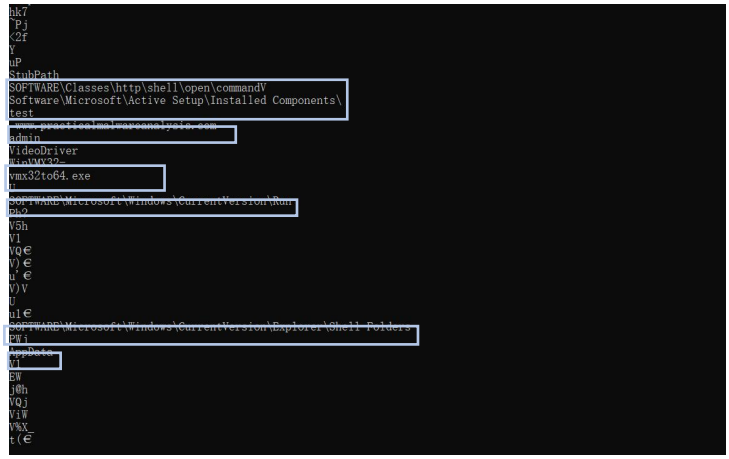
① 用 PEiD 打开 Lab03-01.exe，可以看到 Lab03-01.exe 是加壳的，是 PEncrypt 3.1 Final -> junkcode 的壳。



② 使用 PEview 查看 Lab03-01.exe 的 PE 文件结构和字符串列表，PEview 工具显示该程序导入函数只有 ExitProcess，没有其他导入函数。



③ 使用 strings.exe 查看恶意代码中有哪些字符串。使用命令 strings Lab03-01.exe，如下图所示。



看到了很多的字符串，如注册表位置、域名、WinVMX32、VideoDriver、vmx32to64.exe 等。其中方框标记的内容中包含很多注册表信息、一个域名信息和一个应用程序。

猜测分析可能会通过连接访问该网址下载某些木马文件或者通过 vmx32to64.exe 下载打开某些后门。

（2） 这个恶意代码在主机上的感染迹象特征是什么？

① 使用 RegShot 工具分析注册表变化。

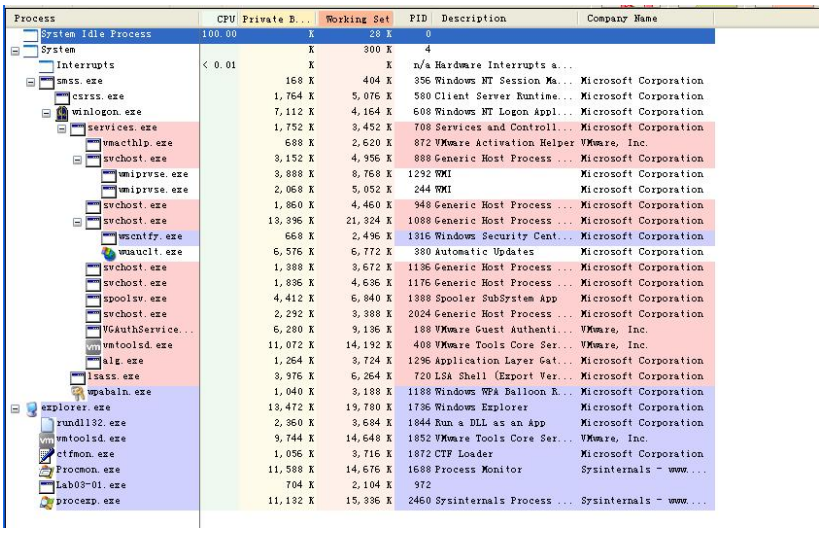
RegShot 是一种注册表比较工具，它通过两次抓取注册表而快速地比较出答案。它还可以将注册表以纯文本方式记录下来，便于浏览；还可以监察 Win.ini，System.ini 中的键值；还可以监察 Windows 目录和 System 目录中文件的变化，为手工卸载某些软件创造条件。通过扫描并保存注册表的“快照”，并对两次快照进行自动的对比，找出快照间存在的不同之处，结果保存成 txt 或者 html 文档。

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver: 43 3A 5C 57 49 4E 44 4F 57 53 5C
HKLM\SYSTEM\ControlSet001\Services\PerfDisk\Performance\WbemAdapFileSignature: 82 4D 6F 69 C8 E9
HKLM\SYSTEM\ControlSet001\Services\PerfDisk\Performance\WbemAdapFileTime: 00 A0 48 BA 4B A1 C8 0
HKLM\SYSTEM\ControlSet001\Services\PerfDisk\Performance\WbemAdapFileSize: 0x00006400
HKLM\SYSTEM\ControlSet001\Services\PerfDisk\Performance\WbemAdapStatus: 0x00000000
HKLM\SYSTEM\ControlSet001\Services\PerfNet\Performance\WbemAdapFileSignature: 06 83 58 0D B1 DD
HKLM\SYSTEM\ControlSet001\Services\PerfNet\Performance\WbemAdapFileTime: 00 A0 48 BA 4B A1 C8 01
HKLM\SYSTEM\ControlSet001\Services\PerfNet\Performance\WbemAdapFileSize: 0x00003E00
HKLM\SYSTEM\ControlSet001\Services\PerfNet\Performance\WbemAdapStatus: 0x00000000
HKLM\SYSTEM\ControlSet001\Services\PerfOS\Performance\WbemAdapFileSignature: 59 6E 4F 8C A6 11 5
HKLM\SYSTEM\ControlSet001\Services\PerfOS\Performance\WbemAdapFileTime: 00 A0 48 BA 4B A1 C8 01
HKLM\SYSTEM\ControlSet001\Services\PerfOS\Performance\WbemAdapFileSize: 0x00005A00
HKLM\SYSTEM\ControlSet001\Services\PerfOS\Performance\WbemAdapStatus: 0x00000000
HKLM\SYSTEM\ControlSet001\Services\PerfProc\Performance\WbemAdapFileSignature: 64 DF B9 8A DD 4E
HKLM\SYSTEM\ControlSet001\Services\PerfProc\Performance\WbemAdapFileTime: 00 A0 48 BA 4B A1 C8 0
HKLM\SYSTEM\ControlSet001\Services\PerfProc\Performance\WbemAdapFileSize: 0x00008200
HKLM\SYSTEM\ControlSet001\Services\PerfProc\Performance\WbemAdapStatus: 0x00000000
HKLM\SYSTEM\ControlSet001\Services\PSched\Performance\WbemAdapFileSignature: 81 A2 82 4E 91 DE F
HKLM\SYSTEM\ControlSet001\Services\PSched\Performance\WbemAdapFileTime: 00 A0 48 BA 4B A1 C8 01
HKLM\SYSTEM\ControlSet001\Services\PSched\Performance\WbemAdapFileSize: 0x00002A00
HKLM\SYSTEM\ControlSet001\Services\PSched\Performance\WbemAdapStatus: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\PerfDisk\Performance\WbemAdapFileSignature: 82 4D 6F 69 C
HKLM\SYSTEM\CurrentControlSet\Services\PerfDisk\Performance\WbemAdapFileTime: 00 A0 48 BA 4B A1
HKLM\SYSTEM\CurrentControlSet\Services\PerfDisk\Performance\WbemAdapFileSize: 0x00006400
HKLM\SYSTEM\CurrentControlSet\Services\PerfDisk\Performance\WbemAdapStatus: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Services\PerfNet\Performance\WbemAdapFileSignature: 06 83 58 0D B1
HKLM\SYSTEM\CurrentControlSet\Services\PerfNet\Performance\WbemAdapFileTime: 00 A0 48 BA 4B A1 C
```

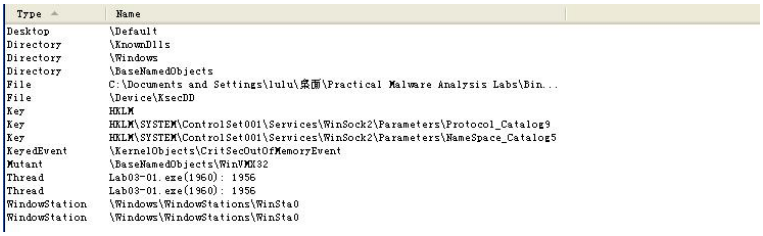
快照比较分析得出该恶意软件在 HKEY_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver 下添加了一个名为-VideoDriver 的自启动项：发现在自启动项 VideoDriver 中增加了键值 43 3A 5C 57 49 4E 44 4F 57 53 5C 73 79 73 74 65 6D 33 32 5C 76 6D 78 33 32 74 6F 36 34 2E 65 78 65，将它换成字符为 C:\WINDOWS\system32\vmx32to64.exe，说明 VideoDriver 自启动项就是指向 system32 目录下的 vmx32to64.exe，程序 vmx32to64.exe 在开机时会自启动。

② 使用 Process explorer 分析

先运行 procmon 工具，并清除所有事件；启动 Process Explorer，同时配置出一个虚拟网络，包括 ApateDNS、Netcat(监听端口 80 和 443),以及用于网络数据包捕获的 Wireshark。

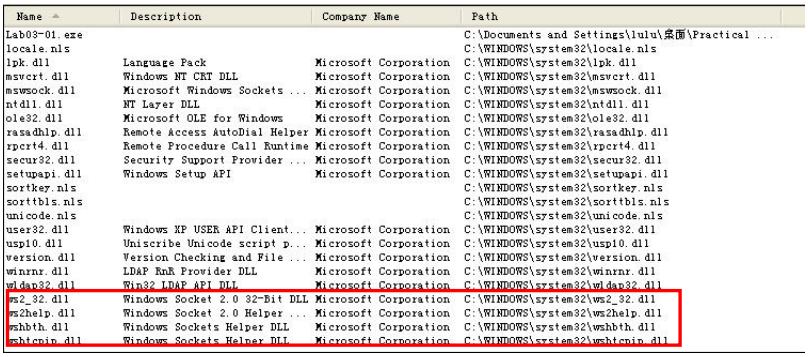


选择 View→Lower Pane View→Handles，可以看到，恶意代码已经创建了一个名为 WinVMX32 的互斥量。



Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\Windows
Directory	\BaseNamedObjects
File	C:\Documents and Settings\lulu\桌面\Practical Malware Analysis Labs\Bin...
File	\Device\KsecDD
Key	HKLM
Key	HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\Protocol_Catalog9
Key	HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\NameSpace_Catalog5
KeyedEvent	\KernelObjects\CritSecOutOfMemoryEvent
Mutant	\BaseNamedObjects\WinMgmt
Thread	Lab03-01.exe(1960): 1956
Thread	Lab03-01.exe(1960): 1956
WindowStation	\Windows\WindowStations\WinSta0
WindowStation	\Windows\WindowStations\WinSta0

选择 View→Lower Pane View→DLL,看到恶意代码动态装载的 DLL 文件。

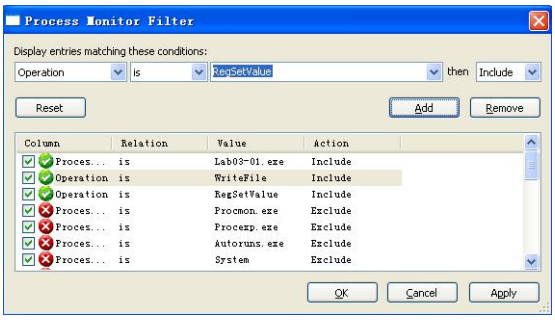


Name	Description	Company Name	Path
Lab03-01.exe			C:\Documents and Settings\lulu\桌面\Practical ...
locale.nls			C:\WINDOWS\system32\locale.nls
lpk.dll	Language Pack	Microsoft Corporation	C:\WINDOWS\system32\lpk.dll
msvcrt.dll	Windows NT CRT DLL	Microsoft Corporation	C:\WINDOWS\system32\msvcrt.dll
mswsock.dll	Microsoft Windows Sockets ...	Microsoft Corporation	C:\WINDOWS\system32\mswsock.dll
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\WINDOWS\system32\ntdll.dll
ole32.dll	Microsoft OLE for Windows	Microsoft Corporation	C:\WINDOWS\system32\ole32.dll
rasadhlp.dll	Remote Access AutoDial Helper	Microsoft Corporation	C:\WINDOWS\system32\rasadhlp.dll
rpcrt4.dll	Remote Procedure Call Runtime	Microsoft Corporation	C:\WINDOWS\system32\rpcrt4.dll
secur32.dll	Security Support Provider ...	Microsoft Corporation	C:\WINDOWS\system32\secur32.dll
setupapi.dll	Windows Setup API	Microsoft Corporation	C:\WINDOWS\system32\setupapi.dll
sortkey.nls			C:\WINDOWS\system32\sortkey.nls
sorttbls.nls			C:\WINDOWS\system32\sorttbls.nls
unicode.nls			C:\WINDOWS\system32\unicode.nls
user32.dll	Windows XP USER API Client...	Microsoft Corporation	C:\WINDOWS\system32\user32.dll
usp10.dll	Uniscribe Unicode script p...	Microsoft Corporation	C:\WINDOWS\system32\usp10.dll
version.dll	Version Checking and File ...	Microsoft Corporation	C:\WINDOWS\system32\version.dll
winrnr.dll	LDAP RnR Provider DLL	Microsoft Corporation	C:\WINDOWS\system32\winrnr.dll
wldap32.dll	Win32 LDAP API DLL	Microsoft Corporation	C:\WINDOWS\system32\wldap32.dll
ws2_32.dll	Windows Socket 2.0 32-Bit DLL	Microsoft Corporation	C:\WINDOWS\system32\ws2_32.dll
ws2help.dll	Windows Socket 2.0 Helper ...	Microsoft Corporation	C:\WINDOWS\system32\ws2help.dll
wshbth.dll	Windows Sockets Helper DLL	Microsoft Corporation	C:\WINDOWS\system32\wshbth.dll
wshtcpip.dll	Windows Sockets Helper DLL	Microsoft Corporation	C:\WINDOWS\system32\wshtcpip.dll

ws2_32.dll 和 wshtcpip.dll 库文件的存在说明该样本存在网络方面的操作。

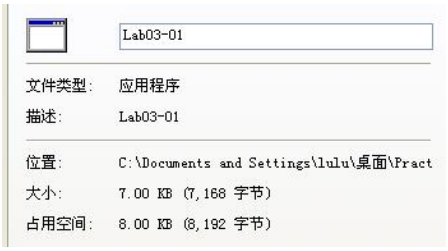
③ 使用 Process Monitor 分析

选择 Filter→Filter,来呼出过滤器对话框，然后设置三个过滤器：一个是对进程名称的过滤(显示 Lab03-01.exe 对系统所做的)，和两个操作上的过滤，包含了 RegSetValue 和 WriteFile，查看恶意代码对文件系统和注册表的修改操作。



设置完过滤器之后，单击 Apply 按钮，便可看到过滤后的结果。显示的条目从数千减少到只有 10 条，其中只有 1 个 WriteFile 操作的条目，并有 9 个关于 RegSetValue 操作的条目。

HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed 键值上的 RegSetValue 操作是典型的噪声。第四条往后都有 Seed，Seed 说明该程序用了随机数，随机数发生器的种子会有软件在注册表中不停地更新。



Process Name	PID	Operation	Path	Result	Detail
Lab03-01.exe	972	RegSetValue	HKLM\SOFTWARE\Microsoft\Crypto...	SUCCESS	Type: REG_BIN...
Lab03-01.exe	972	WriteFile	C:\WINDOWS\system32\vmx32to64.exe	SUCCESS	Offset: 0, Le...
Lab03-01.exe	972	RegSetValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_SZ,...
Lab03-01.exe	972	RegSetValue	HKLM\SOFTWARE\Microsoft\Crypto...	SUCCESS	Type: REG_BIN...
Lab03-01.exe	972	RegSetValue	HKLM\SOFTWARE\Microsoft\Crypto...	SUCCESS	Type: REG_BIN...
Lab03-01.exe	972	RegSetValue	HKLM\SOFTWARE\Microsoft\Crypto...	SUCCESS	Type: REG_BIN...
Lab03-01.exe	972	RegSetValue	HKLM\SOFTWARE\Microsoft\Crypto...	SUCCESS	Type: REG_BIN...
Lab03-01.exe	972	RegSetValue	HKLM\SOFTWARE\Microsoft\Crypto...	SUCCESS	Type: REG_BIN...
Lab03-01.exe	972	RegSetValue	HKLM\SOFTWARE\Microsoft\Crypto...	SUCCESS	Type: REG_BIN...
Lab03-01.exe	972	RegSetValue	HKLM\SOFTWARE\Microsoft\Crypto...	SUCCESS	Type: REG_BIN...

双击 WriteFile 操作条目，显示记录会告诉我们，恶意代码往 C:\WINDOWS\System32\vmx32to64.exe 中写了 7168 字节,恰好是 Lab03-01.exe 文件的大小。

打开 Windows 资源管理器浏览到这个位置，使用 WinMD5 查看 vmx32to64.exe 与 Lab03-01.exe 的 MD5 值，可以看到这个新创建的文件有着与 Lab03-01.exe 相同的 MD5 哈希值，这告诉恶意代码已经复制本身到这个文件系统位置上。这是一个非常有用的感染主机迹象特征，因为它使用了一个硬编码的文件名。

Lab03-01

文件类型: 应用程序
描述: Lab03-01
位置: C:\Documents and Settings\lulu\桌面\Pract
大小: 7.00 KB (7,168 字节)
占用空间: 8.00 KB (8,192 字节)

vmx32to64

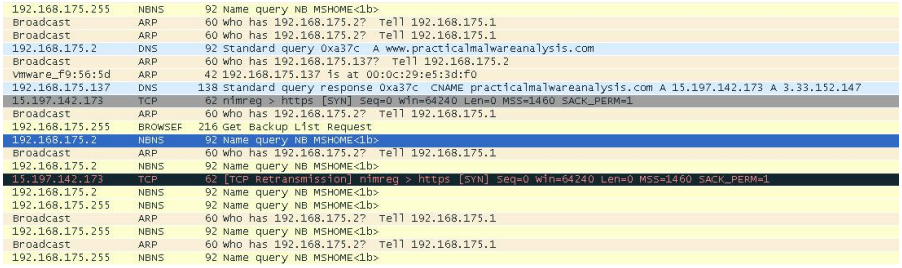
文件类型: 应用程序
描述: vmx32to64
位置: C:\WINDOWS\system32
大小: 7.00 KB (7,168 字节)
占用空间: 8.00 KB (8,192 字节)

双击红框中的第二行，发现恶意代码在 Windows\System32 路径下创建写入来 vmx32to64.exe 文件并且在 CurrentVersion\Run 下创建了 VideoDriver 自启动项键值，用于在系统启动时自动运行 vmx32to64.exe。

综上所述，经过初步分析，可以认为在主机上创建互斥量、尝试复制自身并加入系统自启动项，创建注册表键值等，这些都可以作为其在主机上感染的迹象特征。

（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？

使用 wireshark 进行抓包分析，可以看到如下结果：



出现了网址 www.practicalmalwareanalysis.com。

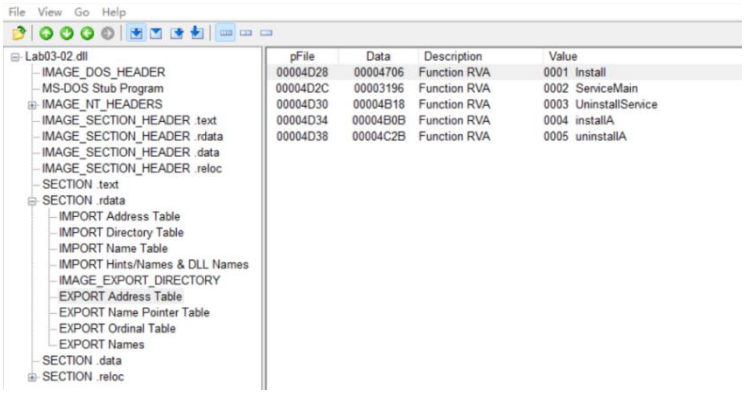
综上所述，Lab03-01.exe 访问了网址 www.practicalmalwareanalysis.com，可以作为网络依据。

（二） Lab3-2

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

（1） 你怎样才能让这个恶意代码自行安装？

使用 PEview 查看 Lab03-02.dll 的导出函数



查看 directory table,发现了一些依赖导入函数动态链接库

a) ADVAPI32.dll：

advapi32.dll 是 Windows 操作系统的一个核心动态链接库文件，包含了很多与系统安全、身份验证、访问控制和注册表操作等相关的函数。该库提

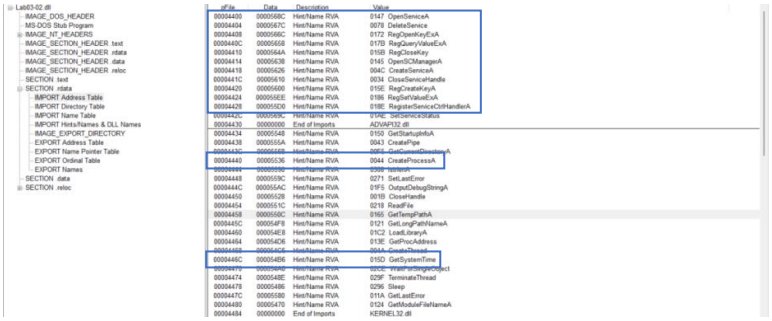
供了一些功能，例如创建和管理用户帐户、验证用户凭据、创建和管理安全上下文、操纵 Windows 服务、管理系统注册表等。

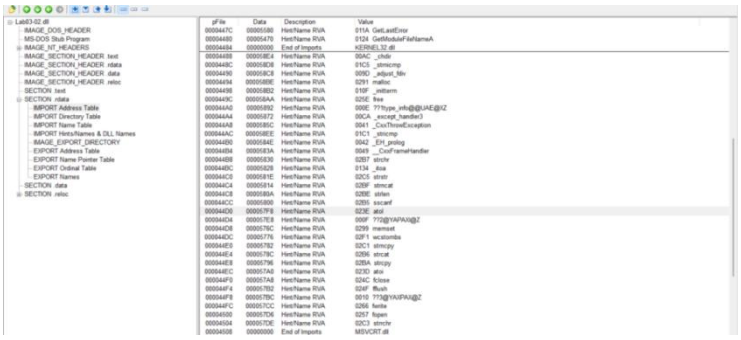
b) MSVCRT.dll:

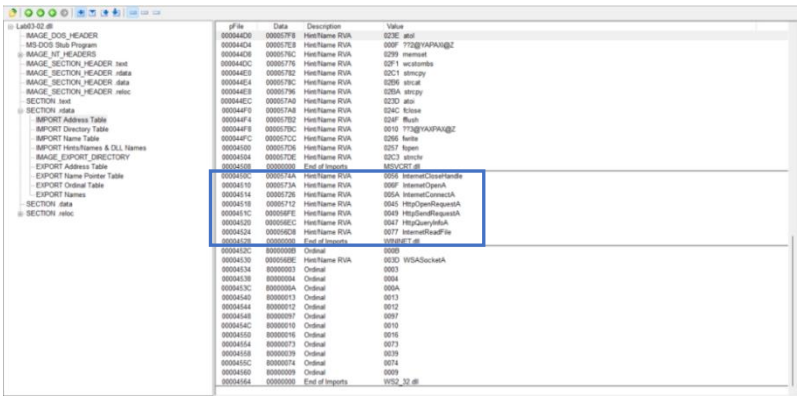
msvcrt.dll 是 windows 操作系统中提供的 C 语言运行库执行文件(Microsoft Visual C Runtime Library)，其中提供了 printf, malloc, strcpy 等 C 语言库函数的具体运行实现，并且为使用 C/C++(Vc)编译的程序提供了初始化（如获取命令行参数）以及退出等功能。

观察 ADVAPI32.dll 依赖的导入函数，发现该恶意代码的功能实现中涉及了开启服务；开启注册表、注册表查询、创建注册表键、设置注册表键值、注册服务控制处理、设置服务状态等。这显然是为了实现 ServiceMain 的正常运行。

查看导入函数，发现程序可以创建进程（CreateProcessA）和线程（CreateThread）服务，创建操控服务（CreateServiceA、OpenServiceA）、操控注册表（RegCreateKeyA、RegSetValueExA、RegisterServiceCtrlHandlerA、RegOpenKeyExA、RegQueryValueExA、RegCloseKey 等），对网络（InternetOpenA、InternetReadFile、InternetConnectA、InternetCloseHandle、HttpOpenRequest、HttpSendRequestA、HttpQueryInfoA 等）进行操作等。







使用 strings Lab03-02.dll 命令进行分析，除去刚才已分析的部分，发现

```
practicalmalwareanalysis.com
serve.html
dW5zdXBwb3J0
c2xlZXA=
Y21k
cXVpdA==
*/*
 Windows XP 6.11
CreateProcessA
kernel32.dll
.exe
GET
HTTP/1.1
%s %s
12345678901234567
quit
exit
getfile
cmd.exe /c
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
--!>
<!--
```

```
CreateService(%s) 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(%s) KEY_QUERY_VALUE success.
RegOpenKeyEx(%s) KEY_QUERY_VALUE error .
SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost
IPRIP
uninstall success
OpenService(%s) error 2
OpenService(%s) error 1
uninstall is starting
.?AVtype_info@@
080@0^0m0r0
```

观察可打印字符串中发现，除了同上发现的一下导入导出函数外，还发现了 practicalmalwareanalysis.com 等一些域名信息、一些注册表信息、IPRIP、serve.html 等字符串，此外还发现了 svchost.exe 的可执行程序。

综上所述，该程序可能通过访问 practicalmalwareanalysis.com 网址，来下载某些程序，将自己下载为某个服务，而 dll 文件在 Windows 系统中一般不可以直接执行，所以必然存在某个可执行程序来运行 Lab03-02.dll 文件，而在可打印字符串中发现的 svchost 很有可能便是运行 dll 文件的 exe

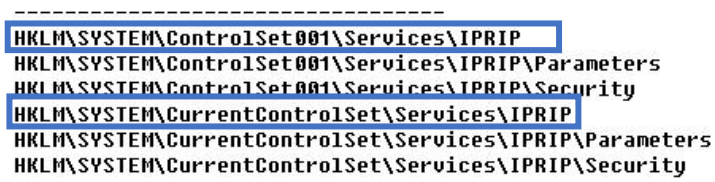
文件。推测这个恶意代码需要使用导出函数 installA 将自身注册为恶意代码分析实战一个服务，我们将使用这个函数来试图安装恶意代码。

根据上述分析可知，可以利用 rundl32.exe 工具，使用命令 rundll32.exe Lab03-02.dll,installA，运行恶意代码导出的 installA 函数，便可将恶意代码安装为一个服务。

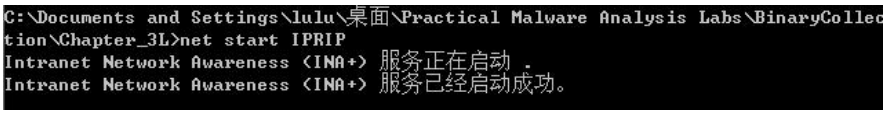
（2） 在安装之后，你如何让这个恶意代码运行起来？

使用 Process Explorer 监控系统上运行的进程。在使用命令 rundll32.exe Lab03-02.dll,installA 运行 Lab03-02.dll 文件前后，分别用 regshot 记录一下注册表信息，点击 compare 对比运行 Lab03-02.dll 的变化。

观察编译后的.txt 文件，在 Keys added 一节中，显示了恶意代码将自身安装为 IPRIP 服务，由于这个恶意代码是个 DLL 文件，它依赖于一个可执行文件来执行它；看到 ImagePath 被设置为 svchost.exe 意味着这个恶意代码将会在一个 swchost.exe 进程中启动。

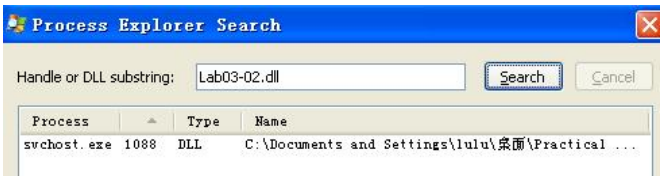


可以看到恶意代码将为自身安装 IPRIP 服务。使用 net start IPRIP 启动服务，就可以成功运行了。



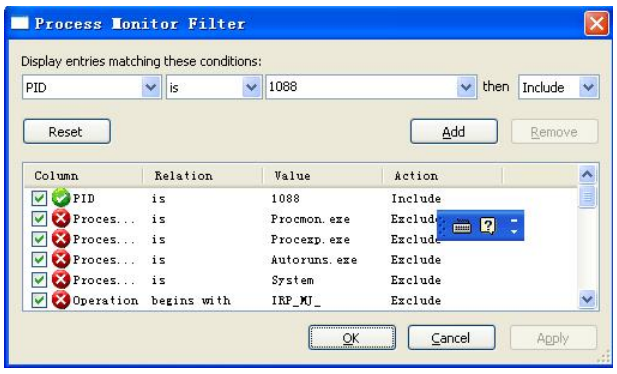
（3） 你怎么能找到这个恶意代码是哪个进程下运行的？

打开 Process Explorer，在里面查找 Lab03-02.dll，发现 Lab03-02.dll 附着在 svchost.exe 上运行，其 pid 为 1088。

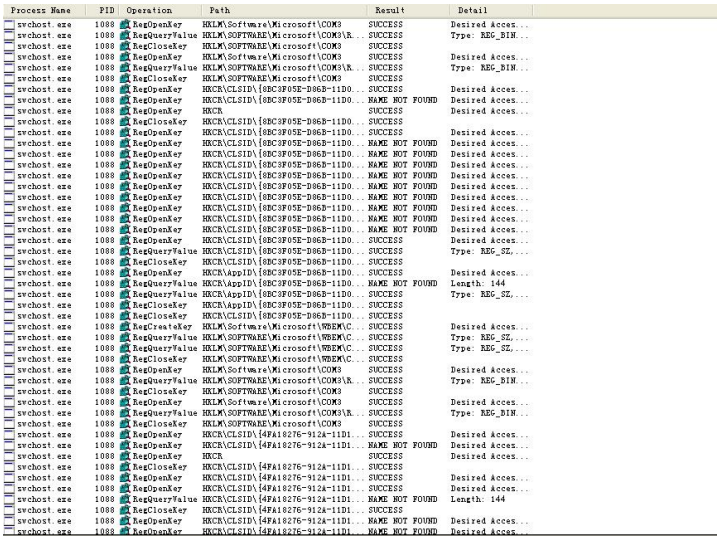


（4） 你可以在 procmon 工具中设置什么样的过滤器，才能收集这个恶意代码的信息？

已知该程序是由 svchost.exe 运行的，并且已经得知了其 PID 为 1088，所以在 Process Monitor 的 filter 使用 Process Explorer 中发现的 PID 作为过滤器。



下面是搜索到的部分结果



（5） 这个恶意代码在主机上的感染迹象特征是什么？

默认情况下，恶意代码将安装为 IPRIP 服务，显示的服务名称为 Intranet Network Awareness(INA+)，它将自身持久地安装在注册表中 HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters\ServiceDl

1:%CurrentDirectory%\Lab03-02.dll，在 Process Explorer 中搜索 DLL 即可查看到 Intranet Network Awareness 这一服务。

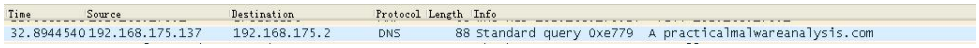
如果将 Lab03-02.dll 重命名为其他文件名，如 malware.dll,然后这个恶意代码就会把 malware.dll 写入到注册表项中。

综上所述，创建 IPRIP 服务可以是这个代码在主机上的感染迹象特征。

（6） 这个恶意代码是否存在一些有用的网络特征码？

查看网络情况，发现了 1088 的端口的网络迹象。

对 Wireshark 的结果进行进一步分析



反映了该程序申请解析域名 practicalmalwareanalysis.com，通过 80 端口连接到这台主机，使用 HTTP 协议，做一个 GET 请求 serve.html,可以作为网络上的一种判断迹象。

（三） Lab3-3

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？

首先使用 Process Explorer 和 procmon 工具。使用 File→Capture Events 将事件捕获先关闭，直到所有动态分析程序都就位，准备好执行恶意代码的时候，再打开开关。用 Filter→Filter 呼出过滤器对话框，然后按一下 Reset 按钮，确保只有默认过滤器被启用。

从命令提示符或双击图标运行 Lab03-03.exe，在 Process Explorer 中观察进程变化。

执行恶意代码，观察 Process Explorer 发现，Lab03-03.exe 刚开始运行几秒钟便退出了，并创建了一个子进程 svchost.exe。过滤 procmon 的结果，分析 Lab03-03.exe 的行为，发现它可以创建进程、加载映像、创建文件、关闭文件等，通过进一步对 operation 的过滤，我们可以发现它确实创建了一个子进程 svchost.exe，PID 为 2768。

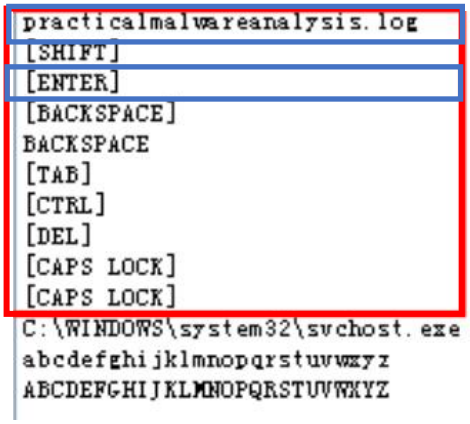
注意到存在大量的 svchost 进程，但瞬间会变为红色，也就是创建子进程 swchost.exe 之后便自动退出，将 svchost.exe 进程继续作为一个“孤儿”进程执行。swchost.exe 作为“孤儿”进程是极不寻常而且是高度可疑的。

（2） 你可以找出任何的内存修改行为嘛？

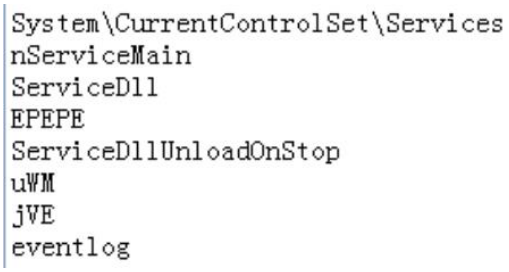
对 svchost.exe"孤儿"进程右击选择 Properties 进行进一步分析，查看它的特征。svchost.exe 文件大小只有 14KB，但在 process explorer 中大小远大于 14KB。

进程看起来像是一个 PID 为 2768 的合法 svchost.exe 进程，但这个 svchost.exe 是很可疑的，因为 svchost.exe 通常是 services.exe 的子进程。

svchost.exe 在 Image 和 Memory 上是非常不同的，Memory 拥有 practicalmalwareanalysis.log、[SHIFT]、[ENTER]等字符，而 Image 中没有。



（Memory 镜像）



（Image 镜像）

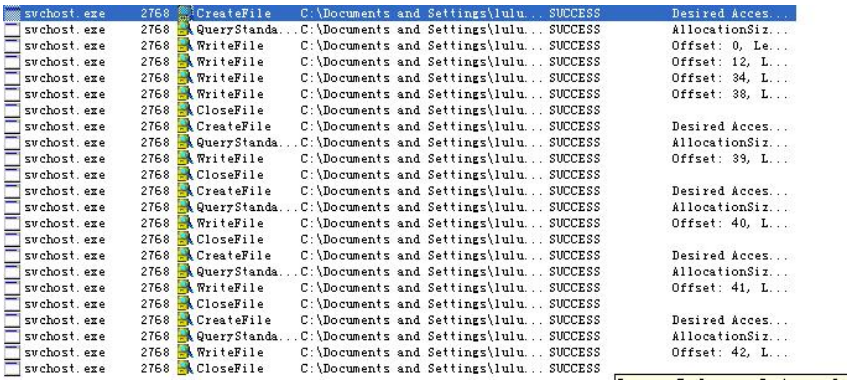
从这个相同的属性页面中，选择 Strings 同时显示在磁盘镜像中和内存镜像中可执行文件的字符串列表。通过在 Image 和 Memory 单选按钮之间切换，可以看出两者镜像中的显著差异。

观察 Memory 镜像框中标出的内容。最上方是一个写入的文件名，然后是一系列键盘符。分析可知，这个程序在尝试创建 practicalmalwareanalysis.log 文件，这就是尝试修改内存的行为。Memory 镜像中蓝框的内容一般不会在磁盘镜像中一个典型的 svchost.exe 文件中出现。磁盘中镜像，确实也没有这样的指令，所以可以判定是恶意代码修改的。

（3） 这个恶意代码在主机上的感染迹象特征是什么？

该恶意软件在 Windows\System32 目录下创建 svchost.exe，且在 Lab03-03.exe 的同一目录下创建了一个 practicalmalwareanalysis.log 日志文件。

practicalmalwareanalysis.log 字符串的存在，再加上出现了[ENTER]、[CAPS LOCK]、[BACKSPACE]等字符串，表明这个程序很可能是一个击键记录器。使用进程 svchost.exe 的在可 Process Explorer 中发现的 PID(2768)在 procmon 工具中创建一个过滤器，并使用过滤器进行过滤，只显示从 PID(2768)进程的事件。



发现 swchostexe 的 CreateFile 和 WriteFile 事件在频繁的写一个名为 practicalmalwareanalysis.log 的文件。它在不断地尝试对自己创建的日志文件 practicalmalwareanalysis.log 进行编辑，这可以作为感染的迹象特征。

（4） 这个恶意代码的目的是什么？

用记事本打开 practicalmalwareanalysis.log,便显示出了刚刚在记事本中输入的击键记录。

这个程序首先创建了一个 svchost.exe 进程，然后就自动退出，可以认为这是尝试在伪装。而其创建的进程试图对原有的进程 svchost.exe 进行替换，实现一个击键记录器。创建 practicalmalwareanalysis.log 文件，内存映像中的字符串信息中会存在大量键盘指令，该文件是为了记录用户对键盘的操作。

（四） Lab3-4

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)

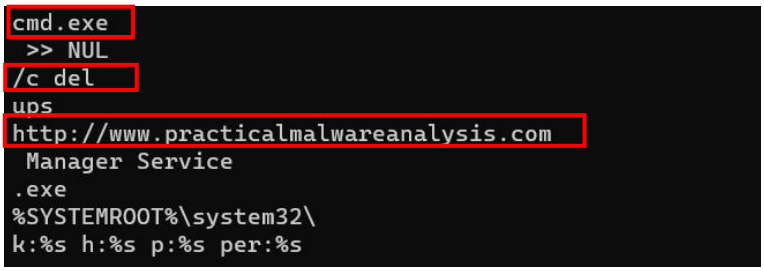
（1） 当你运行这个文件时，会发生什么呢?

当尝试双击打开或者是命令行运行该程序时，发现该程序会打开一个命令行窗口，迅速关掉，最后该程序都会进行自我删除。

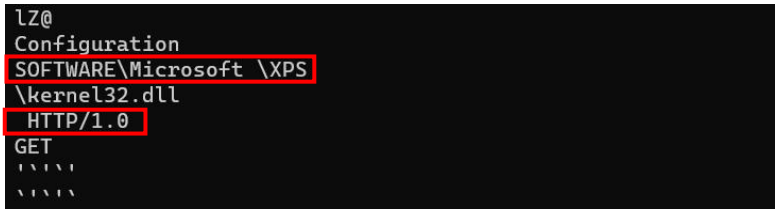
在 Process Explorer 中可以看到，快速运行了 Lab03-04.exe，打开了 cmd.exe，然后进程自己消失。

（2） 是什么原因造成动态分析无法有效实施?

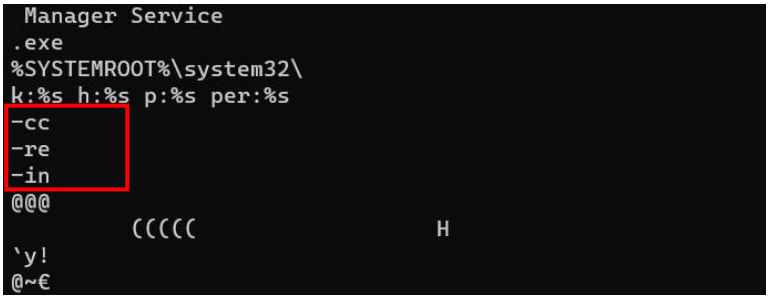
使用 strings Lab03-04.exe 查看字符串，进行静态分析



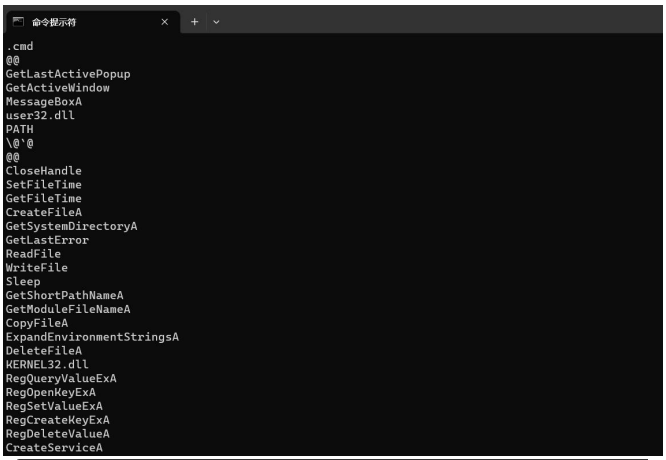
观察到 cmd 命令和 https://www.practicalmalwareanalysis.com 网址，还看到了/c del 删除操作。

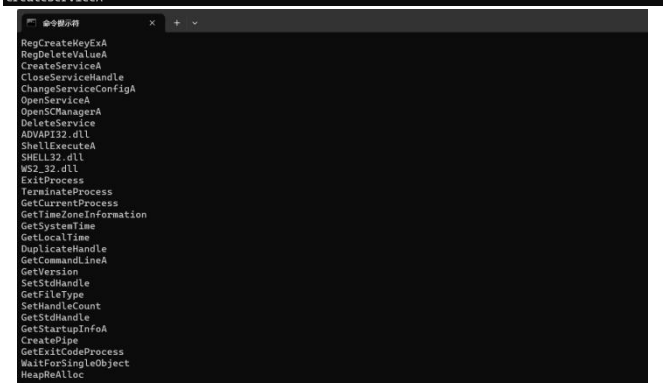


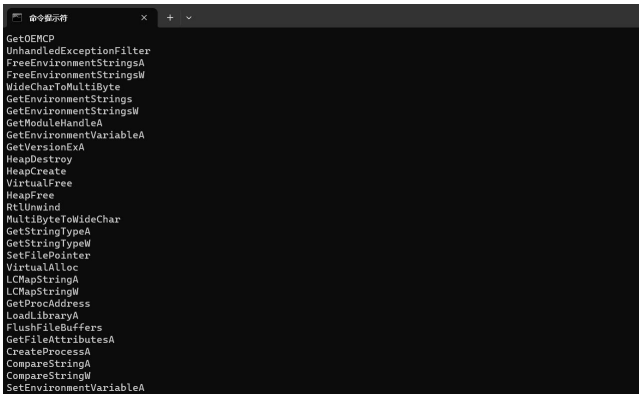
看到域名、注册表位置，如字符串 SOFTWARE\Microsoft \XPS;DOWNLOAD、UPLOAD 这样的命令字符串，以及 HTTP/1.0 字符串等。推测可能是在命令行中运行某些指令，来修改注册表、联网等。这些表明恶意代码可能是一个 HTTP 后门程序。



字符串-cc、-re、-in 应该是一些命令行参数(例如-in 可能是 install 的缩写)。







观察导入函数可知，很多函数与之前的相同，但然没有如 WriteFile、RegSetValue 之类的事件。但是发现了一个 CreateProcessA 及与其相关的条目。分析可知，该恶意代码是通过使用"C:\WINDOWS\system32\cmd.exe"/c del Z:\Lab03-04.exe >> NUL 来从系统中删去自身的。

综上所述，猜测动态分析无法有效实施的原因可能是需要提供一个命令行参数，或者这个程序的某个部件缺失了。

（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-in、-re、-cc，但这样做却没有得到有效的结果，程序还是会删除自身，需要更深入的分析。

四、 实验结论及心得体会

（1） 实验结论

1）恶意代码可以通过修改注册表、创建自启动项、创建互斥量等方式在主机上感染迹象特征。

2）恶意代码可能会通过访问特定的域名或 URL 来与远程服务器通信，这可以作为网络特征码。

3）恶意代码可以创建服务或进程，以隐藏自身并运行在系统中。

4）恶意代码可以修改内存中的内容，如键盘记录器可以记录用户的击键信息。

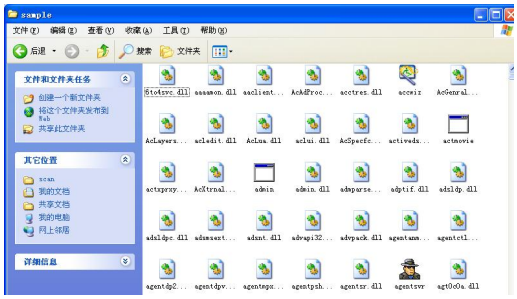
5）有些恶意代码可能会自我删除以避免被检测。

（2） 心得体会

通过本次实验了解了恶意代码分析和感染迹象特征的识别方法。动态分析是一种有力的工具，可以帮助我们理解恶意代码的行为和特征，从而加强网络安全防护和恶意代码防治技术。实验中的工具和技术对于安全专业人员来说是非常重要的，能够帮助我们更好地应对潜在的安全威胁。

（3） 写 yara 规则进行扫描

使用 scan.py 将所有 PE 结构的文件保存到 scan.py 文件所在目录的 sample 文件夹中。



运行结果：

```
C:\Documents and Settings\lulu\桌面\scan>python Lab3.py
样本文件夹中的文件数量：2514
匹配的文件数量：1881
扫描时间：22.42 秒
```

Lab03.py：

```
import os
import yara
import time
# 定义 YARA 规则
rules = yara.compile("Lab03.yara")
# 扫描的样本文件夹路径
sample_folder = "sample"
# 初始化变量
matched_files = 0
start_time = time.time()
# 遍历样本文件夹中的文件
for root, dirs, files in os.walk(sample_folder):
    for file_name in files:
        file_path = os.path.join(root, file_name)
        try:
            # 使用 YARA 规则扫描文件
            matches = rules.match(file_path)
            # 如果有匹配的规则，记录匹配的文件数量
            if matches:
                matched_files += 1
        except Exception as e:
            # 处理可能的异常
            pass  # 这里可以加入处理异常的代码
# 计算扫描时间
```

```
end_time = time.time()
scan_time = end_time - start_time
# 输出结果
print("样本文件夹中的文件数量：{}".format(len(files)))
print("匹配的文件数量：{}".format(matched_files))
print("扫描时间：{:.2f} 秒".format(scan_time))
```

Lab03.yara

```
rule Detect_Lab03 {
    meta:
        description = "YARA rule to detect Lab03 malicious code"
    strings:
        $url = "www.practicalmalwareanalysis.com"
        $registry_key = "HKEY_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\VideoDriver"
        $mutex = "WinVMX32"
        $file_creation = "C:\\WINDOWS\\system32\\vmx32to64.exe"
        $export_function = "installA"
        $svchost_exe = "svchost.exe"
        $practicalmalwareanalysis_log = "practicalmalwareanalysis.log"
        $keyboard_strings = /\\[CTRL]|\\[ENTER\\]|\\[BACKSPACE\\]|\\[TAB\\]|\\[DEL\\]|\\[CAPS LOCK]/
        $cmd = "cmd.exe"
        $del = "/c del"
        $http_string = "HTTP/1.0"
        $command_strings = /DOWNLOAD|UPLOAD/
        $regedit = "SOFTWARE\\Microsoft \\XPS"
    condition:
        any of ($url, $registry_key, $mutex, $file_creation,$export_function,$svchost_exe,$practicalmalwareanalysis_log,$keyboard_strings,$cmd,$del,$http_string,$command_strings,$regedit)
}
```