恶意代码分析与防治技术

Lab 3

动态分析基础技术

2112514 辛浩然

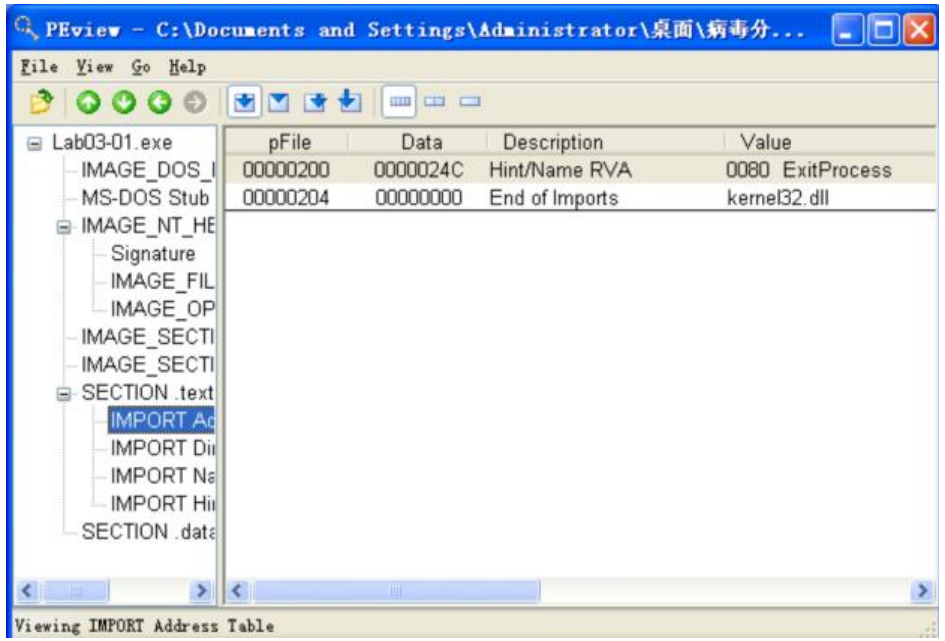
2023 年 10 月 9 日

0 实验环境和实验工具

- 使用VMware 搭建的 Windows XP 虚拟环境，关闭病毒防护
- 静态分析工具：PEView、Strings 、PEiD 等
- 动态分析工具：Process Monitor、Process Explorer、RegShot、ApateDNS、Wireshark 等

Lab1 静态分析

- ◆在PEView中打开恶意代码
  - ◆只有一个导入函数 ExitProcess
- ◆猜测恶意代码加壳或混淆
- ◆使用 PEiD 检测加壳情况信息
  - ◆加壳信息为为 PEncrypt 3.1 Final -> junkcode



Lab1 字符串信息

查看字符串：

- 域名
- 注册表位置
- VideoDriver
- vmx32to64.exe

等字符串

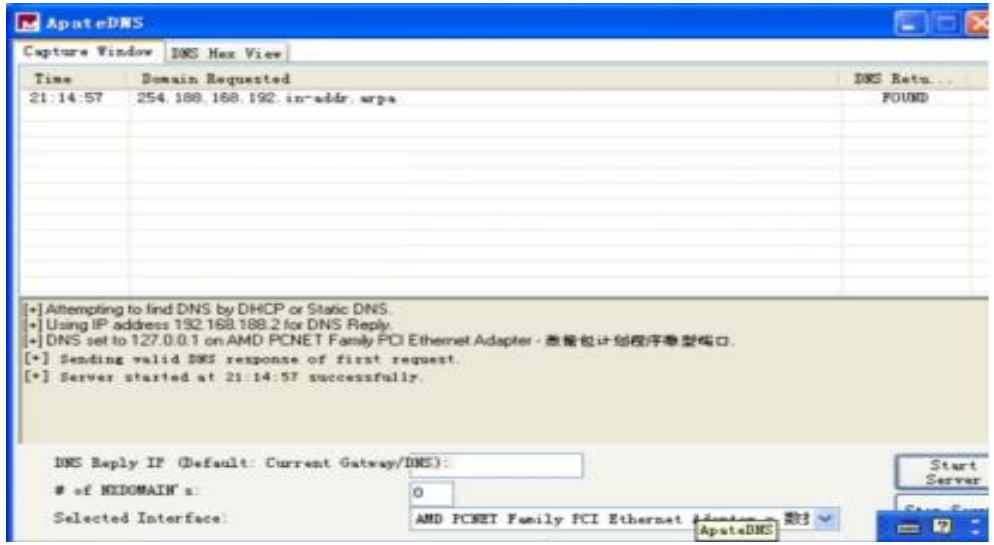
```
C:\WINDOWS\system32\cmd.exe
<2f
Y
uP
StubPath
SOFTWARE\Classes\http\shell\open\commandV
Software\Microsoft\Active Setup\Installed Components\
test
 www.practicalmalwareanalysis.com
admin
VideoDriver
WinVMX32-
vmx32to64.exe
U
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Ph?
V5h
V1
VQÇ
V>Ç
u'Ç
V>V
U
u1Ç
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
PWj
```

Lab1 动态分析环境配置

先运行Process Monitor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；

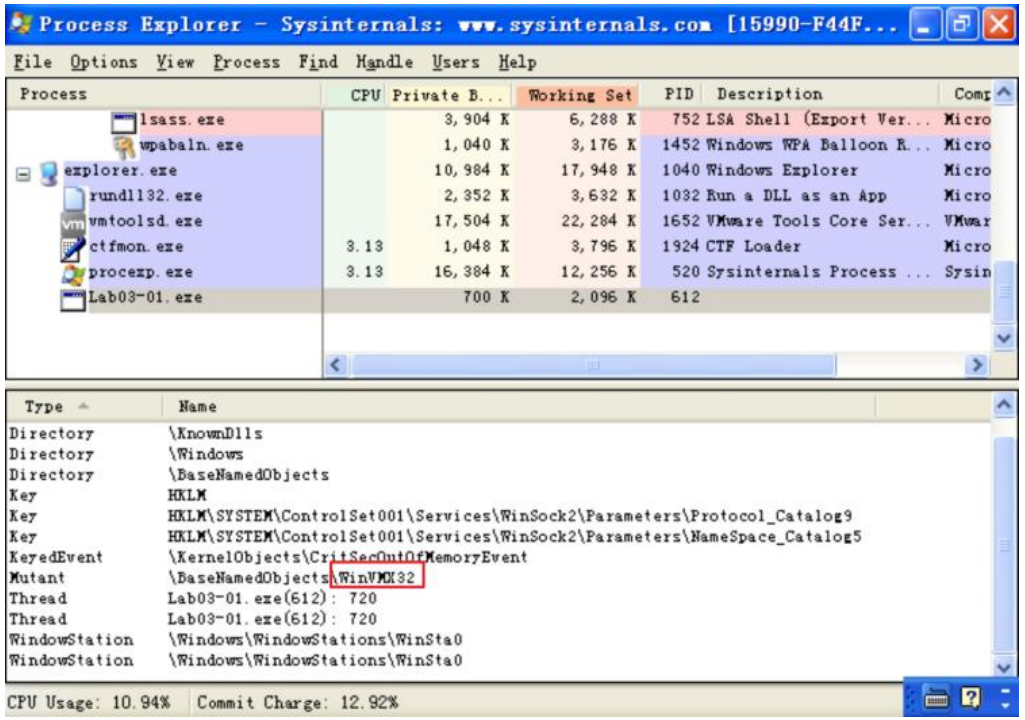
在Regshot中拍摄快照。

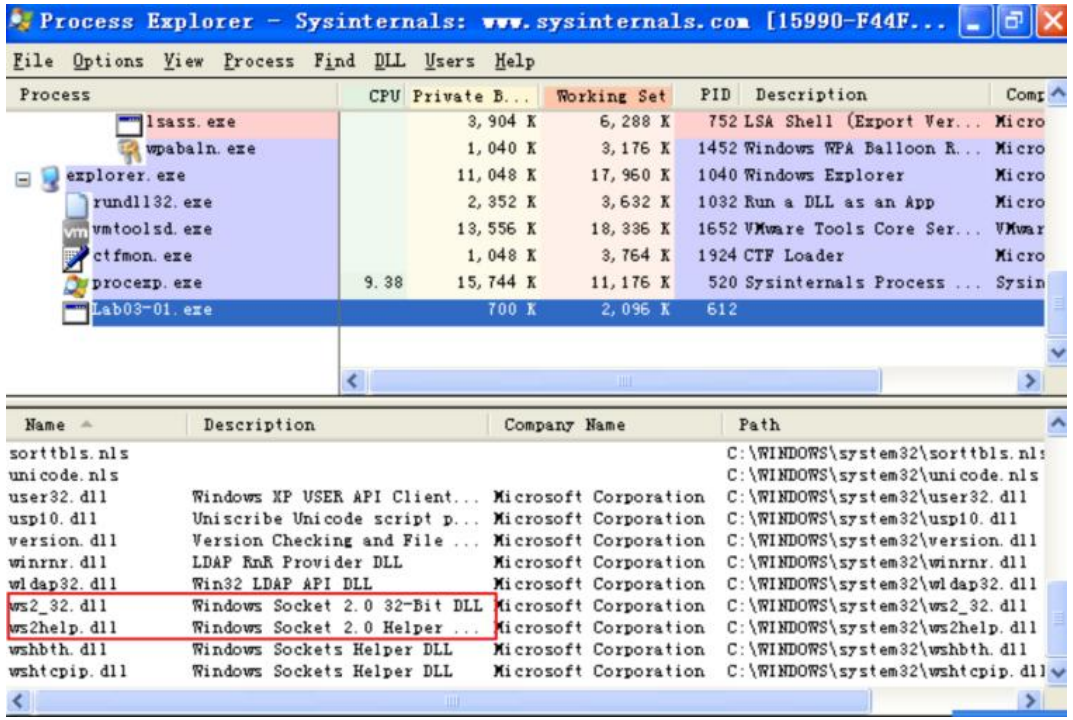


Lab1 Process Explorer 查看运行情况

查看handles：创建了一个名为**WinVMX32**的互斥量；

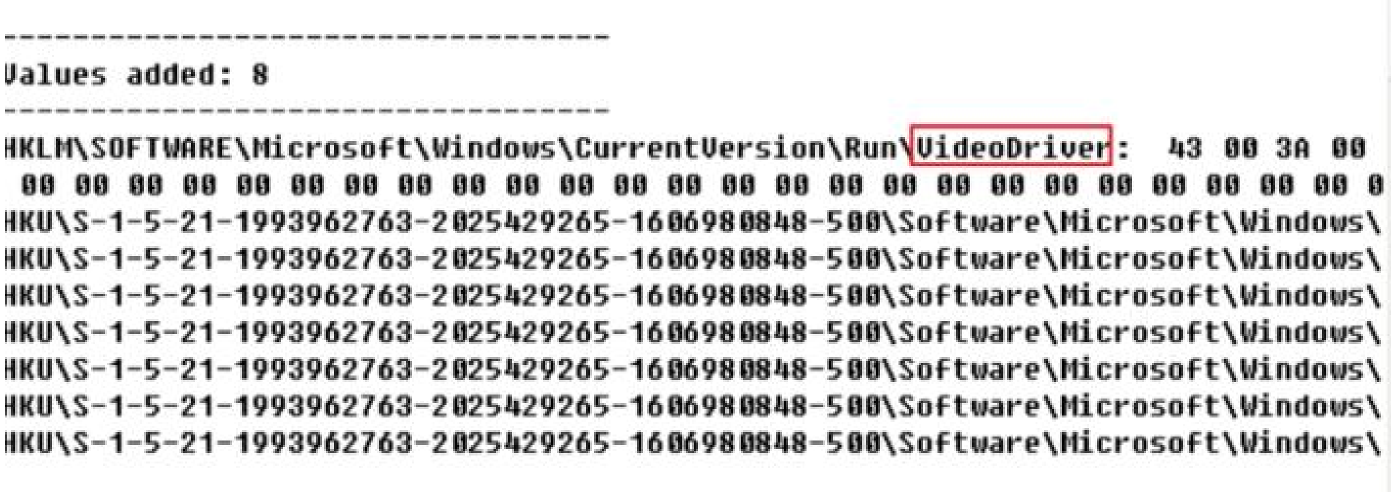
查看动态装载的DLL文件：看到**ws2_32.dll**和**wshtcpip.dll**，这意味着它具有联网功能。





Lab 1 RegShot 快照信息比较

新增
注册表项
Video
Driver



```
----------------------------------
Values added: 8
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver:  43 00 3A 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
HKU\S-1-5-21-1993962763-2025429265-1606980848-500\Software\Microsoft\Windows\
HKU\S-1-5-21-1993962763-2025429265-1606980848-500\Software\Microsoft\Windows\
HKU\S-1-5-21-1993962763-2025429265-1606980848-500\Software\Microsoft\Windows\
HKU\S-1-5-21-1993962763-2025429265-1606980848-500\Software\Microsoft\Windows\
HKU\S-1-5-21-1993962763-2025429265-1606980848-500\Software\Microsoft\Windows\
HKU\S-1-5-21-1993962763-2025429265-1606980848-500\Software\Microsoft\Windows\
HKU\S-1-5-21-1993962763-2025429265-1606980848-500\Software\Microsoft\Windows\
```

```
49 00 4E 00 44 00 4F 00 57 00 53 00 5C 00 73 00 79 00 73 00 74 00 65 00 6
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
on\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_
MUICache\@shell32.dll,-31254: "重命名这个文件夹"
MUICache\@shell32.dll,-31256: "移动这个文件夹"
MUICache\@shell32.dll,-31258: "复制这个文件夹"
MUICache\@shell32.dll,-31380: "以电子邮件形式发送该文件夹内的文件"
MUICache\@shell32.dll,-31262: "删除这个文件夹"
MUICache\C:\Documents and Settings\Administrator\桌面\病毒分析样本\Binary
```

一些
文件操作

Lab 1 Process Monitor

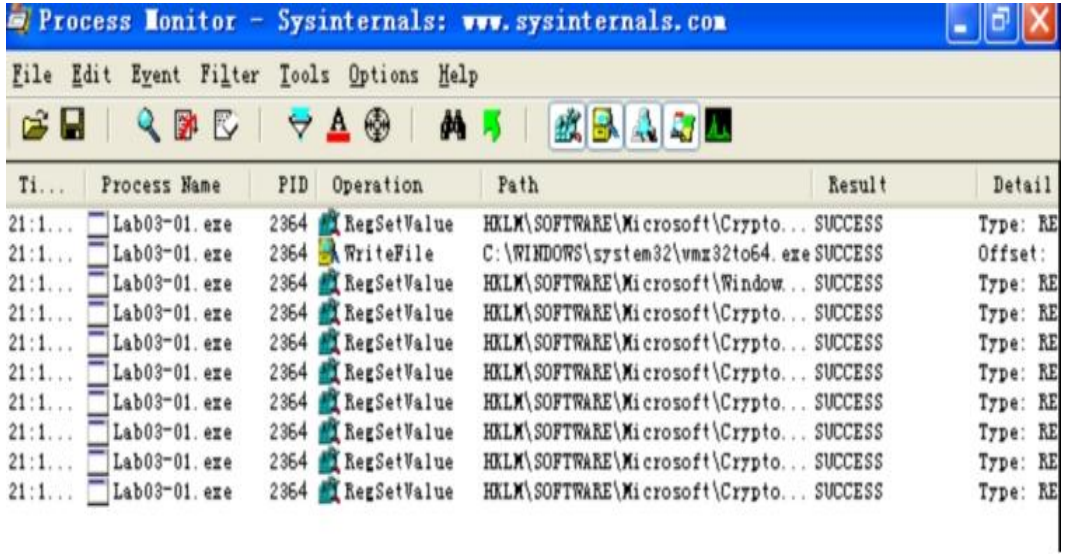
设置三个过滤器：

- ✓ 对进程名称的过滤；
- ✓ 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。

这些记录中有一定数量的噪声：

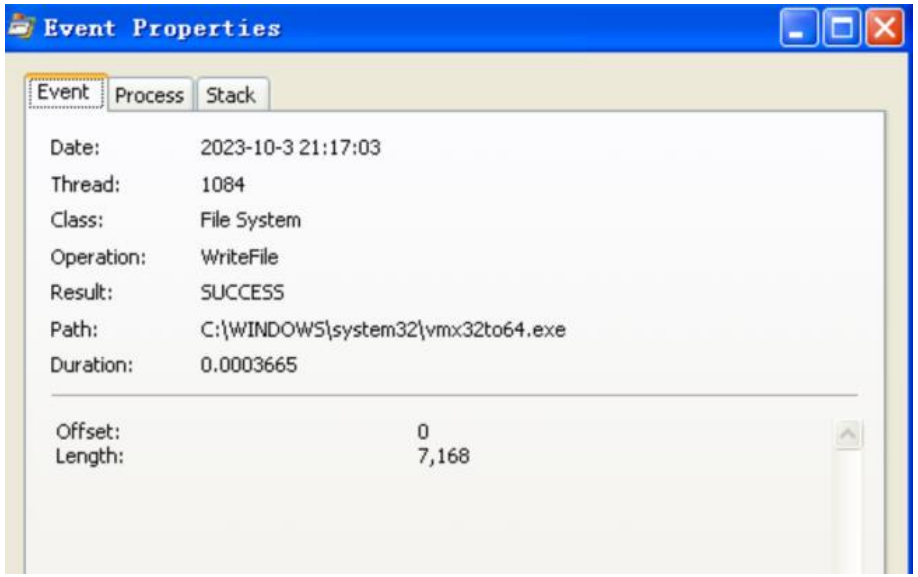
比如LM\SOFTWARE\Microsoft\Cryptography\RNG\Seed键值上的RegSetValue操作是典型的噪声；

因为随机数发生器的种子会有软件在注册表中不停地更新。



Ti...	Process Name	PID	Operation	Path	Result	Detail
21:1...	Lab03-01.exe	2364	RegSetValue	HKLM\SOFTWARE\Microsoft\Crypto...	SUCCESS	Type: RE
21:1...	Lab03-01.exe	2364	WriteFile	C:\WINDOWS\system32\vmx32to64.exe	SUCCESS	Offset:
21:1...	Lab03-01.exe	2364	RegSetValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: RE
21:1...	Lab03-01.exe	2364	RegSetValue	HKLM\SOFTWARE\Microsoft\Crypto...	SUCCESS	Type: RE
21:1...	Lab03-01.exe	2364	RegSetValue	HKLM\SOFTWARE\Microsoft\Crypto...	SUCCESS	Type: RE
21:1...	Lab03-01.exe	2364	RegSetValue	HKLM\SOFTWARE\Microsoft\Crypto...	SUCCESS	Type: RE
21:1...	Lab03-01.exe	2364	RegSetValue	HKLM\SOFTWARE\Microsoft\Crypto...	SUCCESS	Type: RE
21:1...	Lab03-01.exe	2364	RegSetValue	HKLM\SOFTWARE\Microsoft\Crypto...	SUCCESS	Type: RE
21:1...	Lab03-01.exe	2364	RegSetValue	HKLM\SOFTWARE\Microsoft\Crypto...	SUCCESS	Type: RE
21:1...	Lab03-01.exe	2364	RegSetValue	HKLM\SOFTWARE\Microsoft\Crypto...	SUCCESS	Type: RE

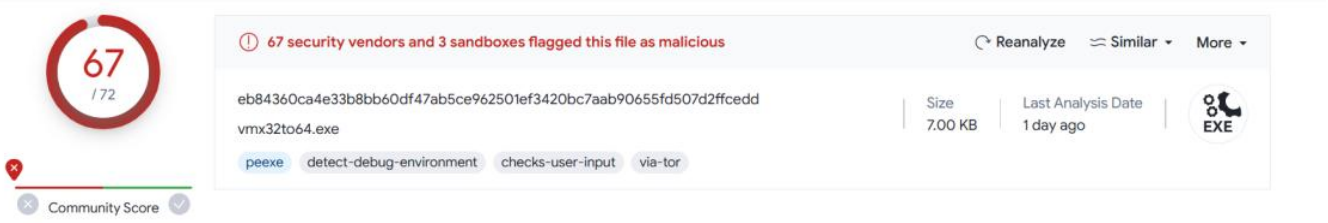
Lab1 WriteFile操作记录

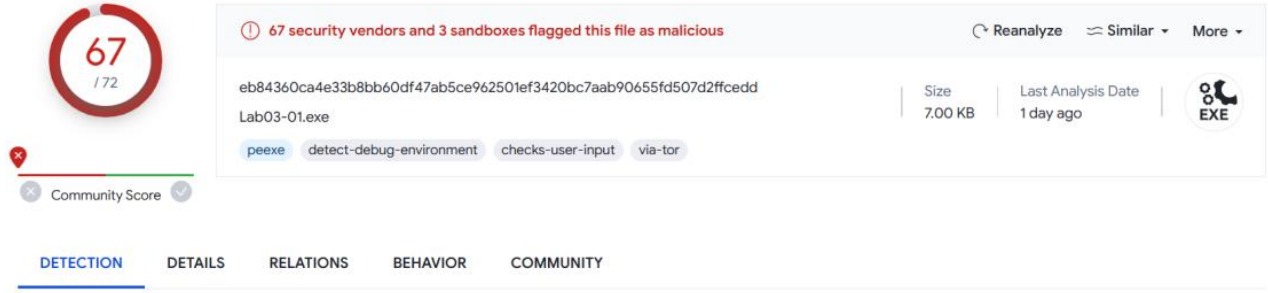


记录显示，恶意代码往C: WINDOWS\System32\vmx32to64.exe中写了7168字节。这恰好是Lab03-01.exe文件的大小。

Lab1 WriteFile操作记录

记录显示，恶意代码往C:WINDOWS\System32\vmx32to64.exe中写了7168字节。这恰好是Lab03-01.exe文件的大小。





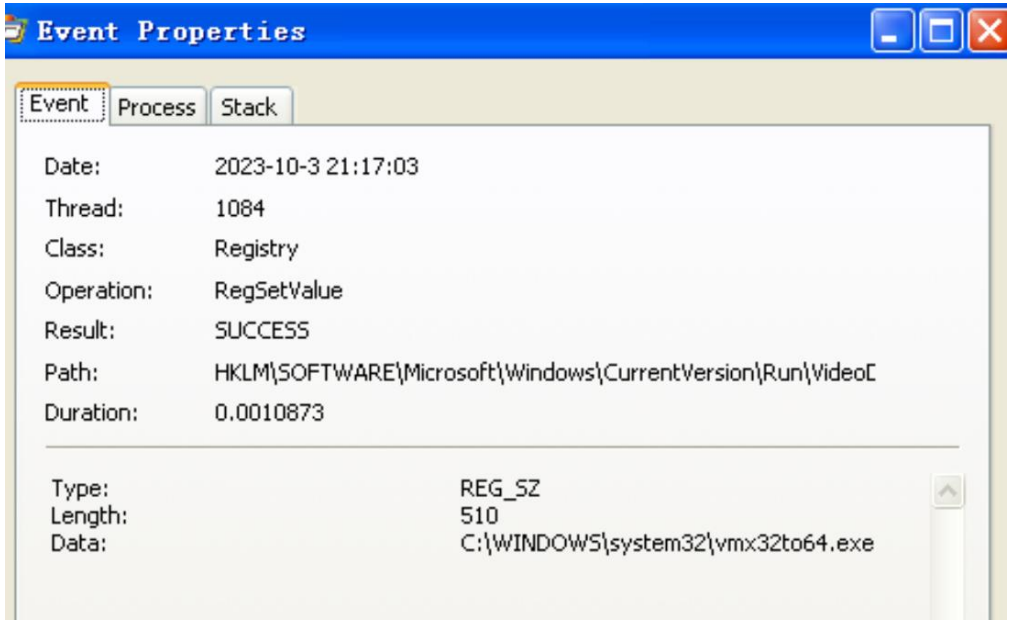
比较新创建的vmx32to64.exe和Lab03-01.exe，可以看到二者具有相同的MD5哈希值，这说明恶意代码已经复制本身到这个文件系统位置上。这是一个非常有用的感染主机迹象特征。

Lab1 RegSetValue 操作记录

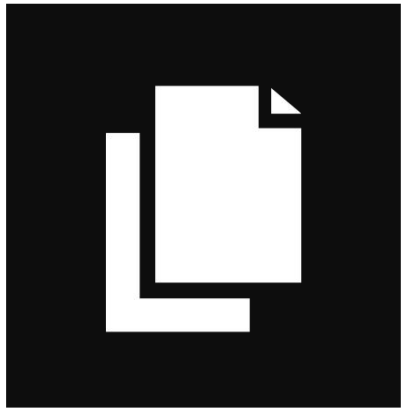
新建了注册表项：

- 位置：HKLM\HKLMI\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- 名称：VideoDriver
- 用于在系统启动时**自动运行**

vmx32to64.exe



Lab1 主机上的感染迹象特征



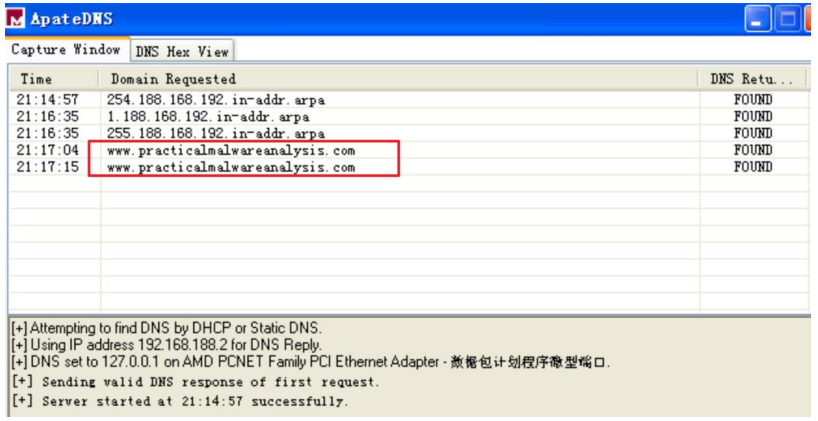
该恶意代码创建了一个名为WinVMX32的互斥量，并复制自身到C:\Windows\System32\vmx32to64.exe

通过创建注册表键值HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver，在系统启动时自动运行vmx32to64.exe

Lab1 网络特征分析

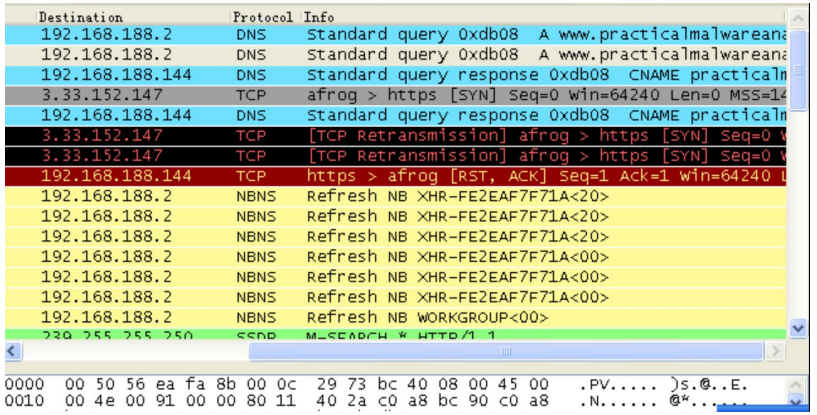
ApateDNS

查看是否执行了DNS请求，可以看到有一个www.practicalmahwareanalysis.com域名的请求



WireShark

说明恶意代码在进行域名解析后，持续地广播大小为256字节的数据包，其中包含看似随机的二进制数据



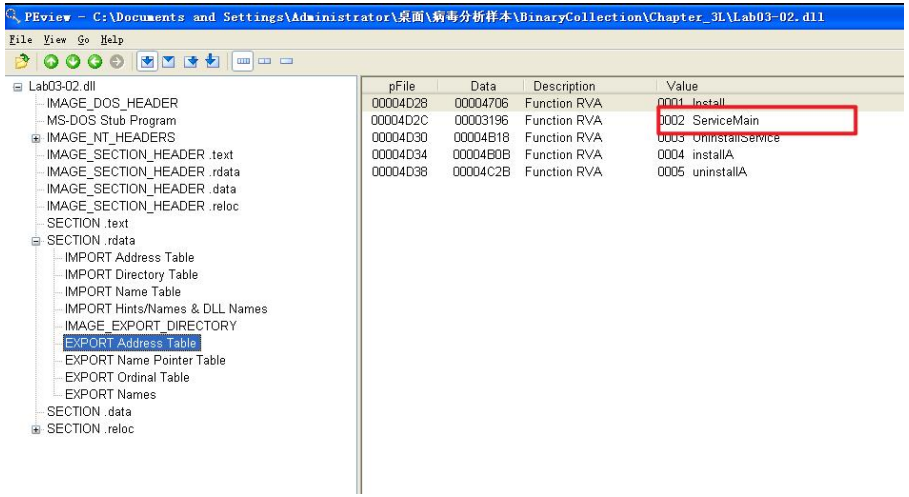
Lab2 静态分析

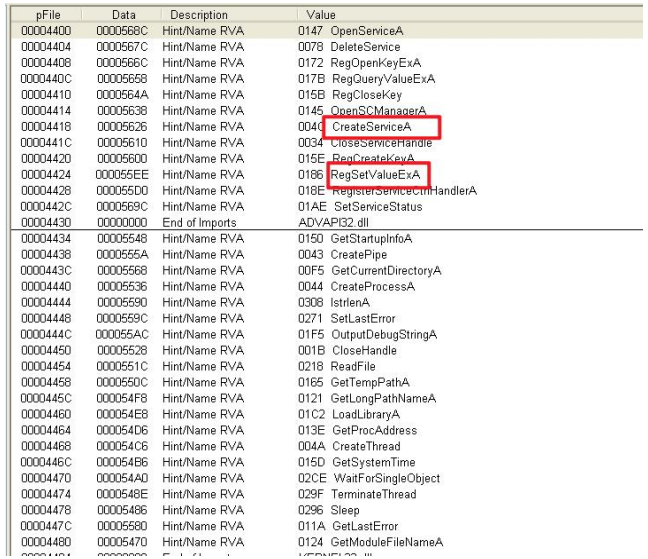
导入表

包括一些服务操作函数，比如CreateService；
注册表操作函数，比如RegSetValueEx；
网络操作函数，比如HttpSendRequest，表明恶意代码使用了HTTP

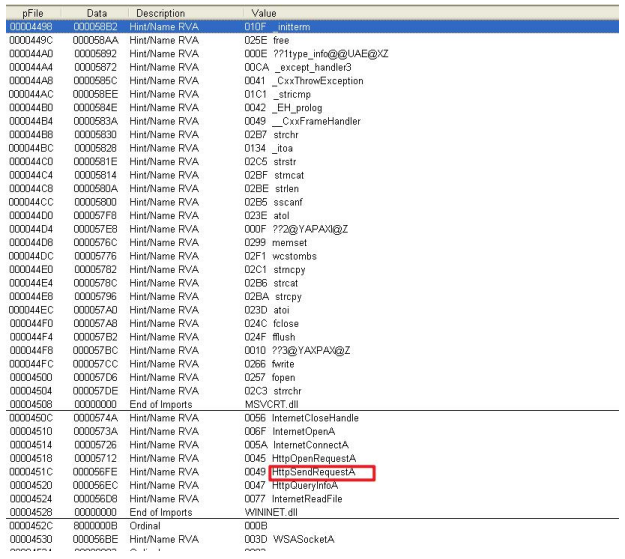
导出表

导出函数ServiceMain表明，恶意代码需要安装一个服务，使其能够正常运行





pFile	Data	Description	Value
00004400	0000568C	Hint/Name RVA	0147 OpenServiceA
00004404	0000567C	Hint/Name RVA	0078 DeleteService
00004408	0000566C	Hint/Name RVA	0172 RegOpenKeyExA
0000440C	00005658	Hint/Name RVA	017B RegQueryValueExA
00004410	0000564A	Hint/Name RVA	015B RegCloseKey
00004414	00005638	Hint/Name RVA	0145 OpenSCManagerA
00004418	00005626	Hint/Name RVA	0040 CreateServiceA
0000441C	00005610	Hint/Name RVA	0034 CloseServiceHandle
00004420	00005600	Hint/Name RVA	015E RegCreateKeyA
00004424	000055EE	Hint/Name RVA	0186 RegSetValueExA
00004428	000055D0	Hint/Name RVA	018E RegisterServiceCtrlHandlerA
0000442C	0000569C	Hint/Name RVA	01AE SetServiceStatus
00004430	00000000	End of Imports	ADVAPI32.dll
00004434	00005548	Hint/Name RVA	0150 GetStartupInfoA
00004438	0000555A	Hint/Name RVA	0043 CreatePipe
0000443C	00005568	Hint/Name RVA	00F5 GetCurrentDirectoryA
00004440	00005536	Hint/Name RVA	0044 CreateProcessA
00004444	00005590	Hint/Name RVA	0308 lstrlenA
00004448	0000559C	Hint/Name RVA	0271 SetLastError
0000444C	000055AC	Hint/Name RVA	01F5 OutputDebugStringA
00004450	00005528	Hint/Name RVA	001B CloseHandle
00004454	0000551C	Hint/Name RVA	0218 ReadFile
00004458	0000550C	Hint/Name RVA	0165 GetTempPathA
0000445C	000054F8	Hint/Name RVA	0121 GetLongPathNameA
00004460	000054E8	Hint/Name RVA	01C2 LoadLibraryA
00004464	000054D6	Hint/Name RVA	013E GetProcAddress
00004468	000054C6	Hint/Name RVA	004A CreateThread
0000446C	000054B6	Hint/Name RVA	015D GetSystemTime
00004470	000054A0	Hint/Name RVA	02CE WaitForSingleObject
00004474	0000548E	Hint/Name RVA	029F TerminateThread
00004478	00005486	Hint/Name RVA	0296 Sleep
0000447C	00005580	Hint/Name RVA	011A GetLastError
00004480	00005470	Hint/Name RVA	0124 GetModuleFileNameA



pFile	Data	Description	Value
00004498	000058B2	Hint/Name RVA	010F __initterm
0000449C	000058AA	Hint/Name RVA	025E free
000044A0	00005892	Hint/Name RVA	000E ??1type_info@@UAE@XZ
000044A4	00005872	Hint/Name RVA	00CA _except_handler3
000044A8	0000585C	Hint/Name RVA	0041 _CxxThrowException
000044AC	000058EE	Hint/Name RVA	01C1 _stricmp
000044B0	0000584E	Hint/Name RVA	0042 _EH_prolog
000044B4	0000583A	Hint/Name RVA	0049 __CxxFrameHandler
000044B8	00005830	Hint/Name RVA	02B7 strchr
000044BC	00005828	Hint/Name RVA	0134 _itoa
000044C0	0000581E	Hint/Name RVA	02C5 strstr
000044C4	00005814	Hint/Name RVA	02BF strncat
000044C8	0000580A	Hint/Name RVA	02BE strlen
000044CC	00005800	Hint/Name RVA	02B5 sscanf
000044D0	000057F8	Hint/Name RVA	023E atol
000044D4	000057E8	Hint/Name RVA	000F ??2@YAPAXI@Z
000044D8	0000576C	Hint/Name RVA	0299 memset
000044DC	00005776	Hint/Name RVA	02F1 wcstombs
000044E0	00005782	Hint/Name RVA	02C1 strncpy
000044E4	0000578C	Hint/Name RVA	02B6 strcat
000044E8	00005796	Hint/Name RVA	02BA strcpy
000044EC	000057A0	Hint/Name RVA	023D atoi
000044F0	000057A8	Hint/Name RVA	024C fclose
000044F4	000057B2	Hint/Name RVA	024F fflush
000044F8	000057BC	Hint/Name RVA	0010 ??3@YAXPAX@Z
000044FC	000057CC	Hint/Name RVA	0266 fwrite
00004500	000057D6	Hint/Name RVA	0257 fopen
00004504	000057DE	Hint/Name RVA	02C3 strrchr
00004508	00000000	End of Imports	MSVCRT.dll
0000450C	0000574A	Hint/Name RVA	0056 InternetCloseHandle
00004510	0000573A	Hint/Name RVA	006F InternetOpenA
00004514	00005726	Hint/Name RVA	005A InternetConnectA
00004518	00005712	Hint/Name RVA	0045 HttpOpenRequestA
0000451C	000056FE	Hint/Name RVA	0049 HttpSendRequestA
00004520	000056EC	Hint/Name RVA	0047 HttpQueryInfoA
00004524	000056D8	Hint/Name RVA	0077 InternetReadFile
00004528	00000000	End of Imports	WININET.dll
0000452C	8000000B	Ordinal	000B
00004530	000056BE	Hint/Name RVA	003D WSASocketA

Lab2 字符串信息

可以发现一些**注册表位置**、域名、IPRIP、serve.html等字符串

```
__CxxFrameHandler
_EH_prolog
_CxxThrowException
_except_handler3
MSVCRT.dll
??1type_info@@UAE@XZ
free
_initterm
malloc
_adjust_fdiv
_strnicmp
_chdir
_stricmp
Lab03-02.dll
Install
ServiceMain
UninstallService
installA
uninstallA
Y29ubmVjdA==
practicalmalwareanalysis.com
serve.html
[illegible]
c2xlZXA=
Y21k
cXVpdA==
*/*
 Windows XP 6.11
CreateProcessA
kernel32.dll
.exe
GET
HTTP/1.1
%s %s
1234567890123456
quit
exit
getfile
cmd.exe /c
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
-->
<!--
.PAX
.PAD
DependOnService
RpcSs
ServiceDll
GetModuleFileName() get dll path
Parameters
Type
```

Lab2 动态运行恶意代码

通过静态分析，可以发现恶意代码需要使用导出函数installA将自身注册为一个服务。安装前先使用regshot拍摄快照，然后利用rundll32.exe工具，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。

```
C:\Documents and Settings\Administrator\桌面\病毒分析样本\BinaryCollection\Chapt
er_3L>Rundll32.exe Lab03-02.dll,installA
```

安装后再拍摄快照，进行比较

Created with Regshot 1.9.0 x86 Unicode

Comments:

Datetime: 2023/10/4 06:13:13 , 2023/10/4 06:13:55

Computer: XHR-FE2EAF7F71A , XHR-FE2EAF7F71A

Username: Administrator , Administrator

Keys added: 6

HKLM\SYSTEM\ControlSet001\Services\IPRIP
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security

Values added: 20

HKLM\SYSTEM\ControlSet001\Services\IPRIP\Type: 0x00000020
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k netsvcs"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DisplayName: "Intranet Network Awareness (INA+)"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ObjectName: "LocalSystem"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Description: "Depends INA+, Collects and stores network configuration and location information, and notifies applications when this information changes."
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DependOnService: 52 00 70 00 63 00 53 00 73 00 00 00 00 00
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters\ServiceDll: "C:\Documents and Settings\Administrator\Lhb?\ŵ¢-R?g7h,g\BinaryCollection\Chapter_3L\Lab03-02.dll"
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
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Type: 0x00000020
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Start: 0x00000002
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ErrorControl: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k netsvcs"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\DisplayName: "Intranet Network Awareness (INA+)"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ObjectName: "LocalSystem"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Description: "Depends INA+, Collects and stores network configuration and location information, and notifies applications when this information changes."
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\DependOnService: 52 00 70 00 63 00 53 00 73 00 00 00 00 00
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters\ServiceDll: "C:\Documents and Settings\Administrator\Lhb?\ŵ¢-R?g7h,g\BinaryCollection\Chapter_3L\Lab03-02.dll"
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

Lab2 动态运行恶意代码

安装后再拍摄快照，进行比较

- Keys added中显示了恶意代码将自身安装为**IPRIP服务**；
- ImagePath被设置为svchost.exe，这意味着这个恶意代码将会在一个swchost.exe进程中启动；
- 其余的信息，比如DisplayName和Description。可以作为识别这个恶意服务的独特指纹特征。

Created with Regshot 1.9.0 x86 Unicode

Comments:

Datetime: 2023/10/4 06:13:13 , 2023/10/4 06:13:55

Computer: XHR-FE2EAF7F71A , XHR-FE2EAF7F71A

Username: Administrator , Administrator

Keys added: 6

```
HKLM\SYSTEM\ControlSet001\Services\IPRIP
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security
```

Values added: 20

```
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Type: 0x00000020
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k netsvcs"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DisplayName: "Intranet Network Awareness (INA+)"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ObjectName: "LocalSystem"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Description: "Depends INA+, Collects and stores network configuration and loca
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DependOnService: 52 00 70 00 63 00 53 00 73 00 00 00 00 00
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters\ServiceDll: "C:\Documents and Settings\Administrator\Lhb?\ŵ¢-R?g
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 0
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Type: 0x00000020
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Start: 0x00000002
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ErrorControl: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k netsvcs"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\DisplayName: "Intranet Network Awareness (INA+)"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\ObjectName: "LocalSystem"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Description: "Depends INA+, Collects and stores network configuration and
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\DependOnService: 52 00 70 00 63 00 53 00 73 00 00 00 00 00
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters\ServiceDll: "C:\Documents and Settings\Administrator\Lhb?\ŵ¢-
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security\Security: 01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 0
```

Lab2 动态运行恶意代码

安装后再拍摄快照，进行比较

- Keys added中显示了恶意代码将自身安装为**IPRIP服务**；
- ImagePath被设置为svchost.exe，这意味着这个恶意代码将会在一个swchost.exe进程中启动；
- 其余的信息，比如DisplayName和Description。可以作为识别这个恶意服务的独特指纹特征。

主机上的感染迹象

- 恶意代码将安装为IPRIP服务
- 显示的服务名称为Intranet Network Awareness(INA+)
- 描述为"Depends INA+, Collects and stores network configuration and location information, and notifies applications when this information changes"
- 它将自身持久地安装在注册表中

Lab2 动态运行恶意代码

由于恶意代码安装为IPRIP服务，启动IPRIP服务，运行恶意代码

```
C:\Documents and Settings\Administrator>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。
```

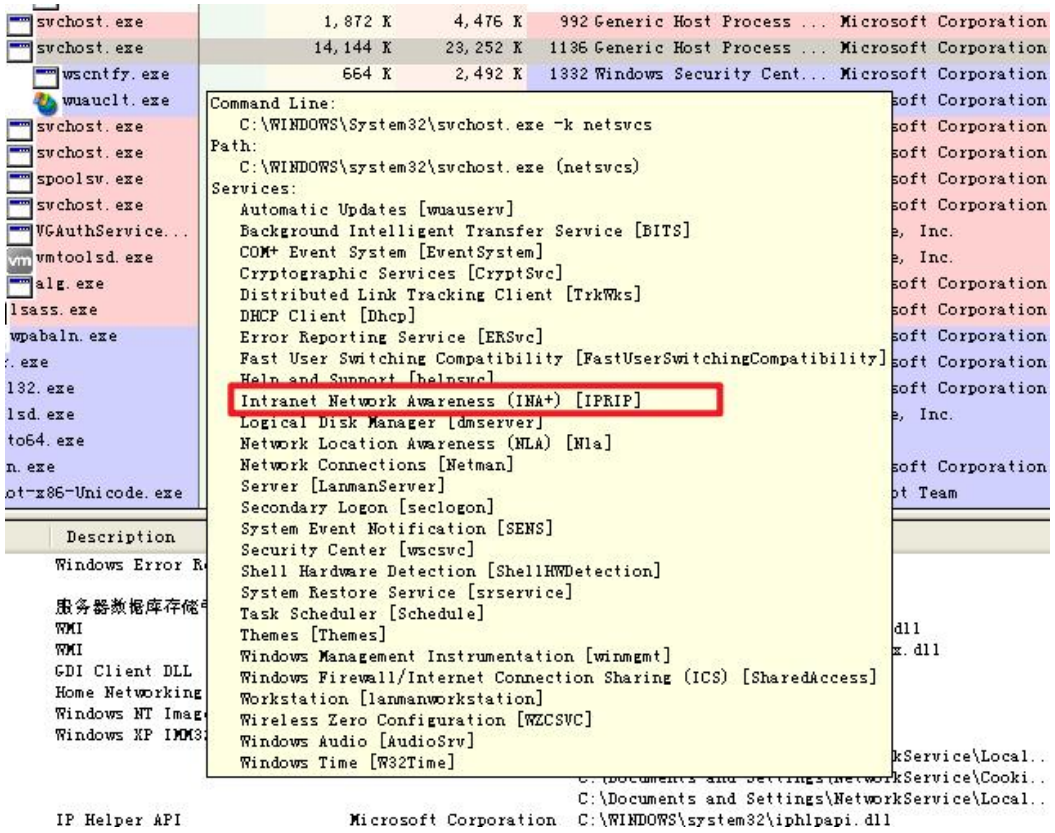
打开 Process Explorer，使用FIND DLL功能寻找恶意代码运行的进程

Lab03-02.dll是由PID为1136的svchost.exe进程加载的

Lab2 动态运行恶意代码

在该进程的服务中可以看到IPRIP，证实了恶意代码在svchost.exe进程中运行

Services



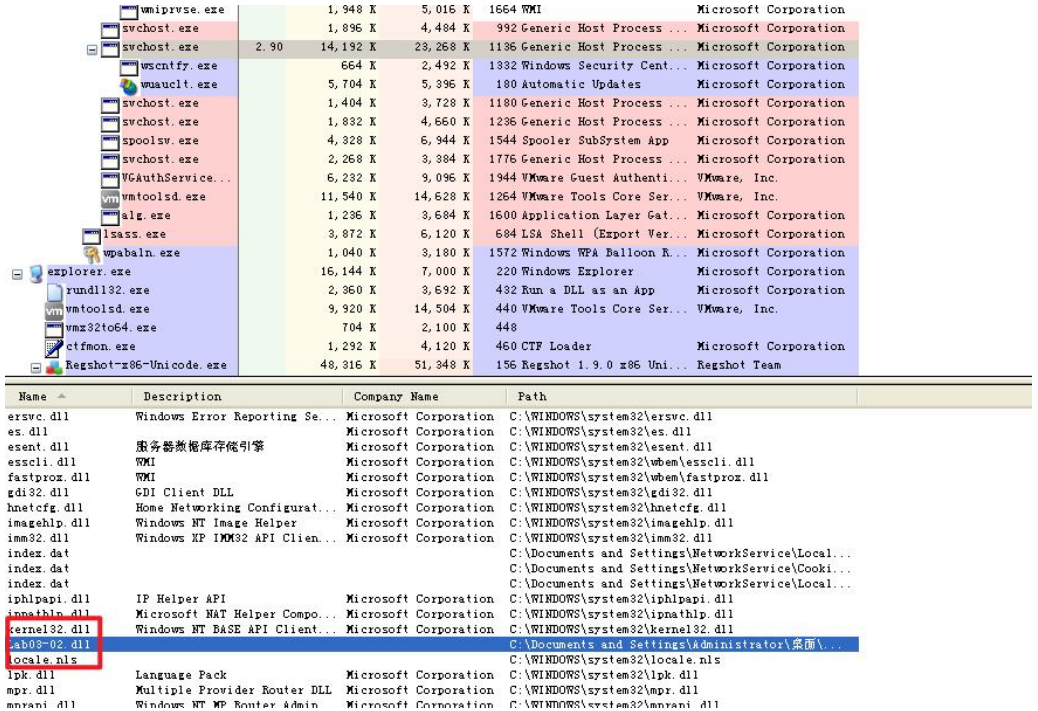
Lab2 动态运行恶意代码

在该进程的服务中可以看到IPRIP，证实了恶意代码<u>在svchost.exe进程中运行</u>

Services

DLL

可以看到Lab03--02.dll被装载



wmiprvse.exe		1,948 K	5,016 K	1664	WMI	Microsoft Corporation
svchost.exe		1,896 K	4,484 K	992	Generic Host Process ...	Microsoft Corporation
svchost.exe	2.90	14,192 K	23,268 K	1136	Generic Host Process ...	Microsoft Corporation
wscntfy.exe		664 K	2,492 K	1332	Windows Security Cent...	Microsoft Corporation
wuauclt.exe		5,704 K	5,396 K	180	Automatic Updates	Microsoft Corporation
svchost.exe		1,404 K	3,728 K	1180	Generic Host Process ...	Microsoft Corporation
svchost.exe		1,832 K	4,660 K	1236	Generic Host Process ...	Microsoft Corporation
spoolsv.exe		4,328 K	6,944 K	1544	Spooler SubSystem App	Microsoft Corporation
svchost.exe		2,268 K	3,384 K	1776	Generic Host Process ...	Microsoft Corporation
VGAuthService...		6,232 K	9,096 K	1944	VMware Guest Authenti...	VMware, Inc.
vmtoolsd.exe		11,540 K	14,628 K	1264	VMware Tools Core Ser...	VMware, Inc.
alg.exe		1,236 K	3,684 K	1600	Application Layer Gat...	Microsoft Corporation
lsass.exe		3,872 K	6,120 K	684	LSA Shell (Export Ver...	Microsoft Corporation
wpabaln.exe		1,040 K	3,180 K	1572	Windows WPA Balloon R...	Microsoft Corporation
explorer.exe		16,144 K	7,000 K	220	Windows Explorer	Microsoft Corporation
rundll32.exe		2,360 K	3,692 K	432	Run a DLL as an App	Microsoft Corporation
vmtoolsd.exe		9,920 K	14,504 K	440	VMware Tools Core Ser...	VMware, Inc.
vmx32to64.exe		704 K	2,100 K	448		
ctfmon.exe		1,292 K	4,120 K	460	CTF Loader	Microsoft Corporation
Regshot-x86-Unicode.exe		48,316 K	51,348 K	156	Regshot 1.9.0 x86 Uni...	Regshot Team

Name	Description	Company Name	Path
erswc.dll	Windows Error Reporting Se...	Microsoft Corporation	C:\WINDOWS\system32\erswc.dll
es.dll		Microsoft Corporation	C:\WINDOWS\system32\es.dll
esent.dll	服务器数据库存储引擎	Microsoft Corporation	C:\WINDOWS\system32\esent.dll
esscli.dll	WMI	Microsoft Corporation	C:\WINDOWS\system32\wbem\esscli.dll
fastprox.dll	WMI	Microsoft Corporation	C:\WINDOWS\system32\wbem\fastprox.dll
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\WINDOWS\system32\gdi32.dll
hnetcfg.dll	Home Networking Configurat...	Microsoft Corporation	C:\WINDOWS\system32\hnetcfg.dll
imagehlp.dll	Windows NT Image Helper	Microsoft Corporation	C:\WINDOWS\system32\imagehlp.dll
imm32.dll	Windows XP IMM32 API Clien...	Microsoft Corporation	C:\WINDOWS\system32\imm32.dll
index.dat			C:\Documents and Settings\NetworkService\Local...
index.dat			C:\Documents and Settings\NetworkService\Cooki...
index.dat			C:\Documents and Settings\NetworkService\Local...
iphlpapi.dll	IP Helper API	Microsoft Corporation	C:\WINDOWS\system32\iphlpapi.dll
ipnathlp.dll	Microsoft NAT Helper Compo...	Microsoft Corporation	C:\WINDOWS\system32\ipnathlp.dll
kernel32.dll	Windows NT BASE API Client...	Microsoft Corporation	C:\WINDOWS\system32\kernel32.dll
Lab03-02.dll			C:\Documents and Settings\Administrator\桌面\...
locale.nls			C:\WINDOWS\system32\locale.nls
lpk.dll	Language Pack	Microsoft Corporation	C:\WINDOWS\system32\lpk.dll
mpr.dll	Multiple Provider Router DLL	Microsoft Corporation	C:\WINDOWS\system32\mpr.dll
mprapi.dll	Windows NT MP Router Admin	Microsoft Corporation	C:\WINDOWS\system32\mprapi.dll

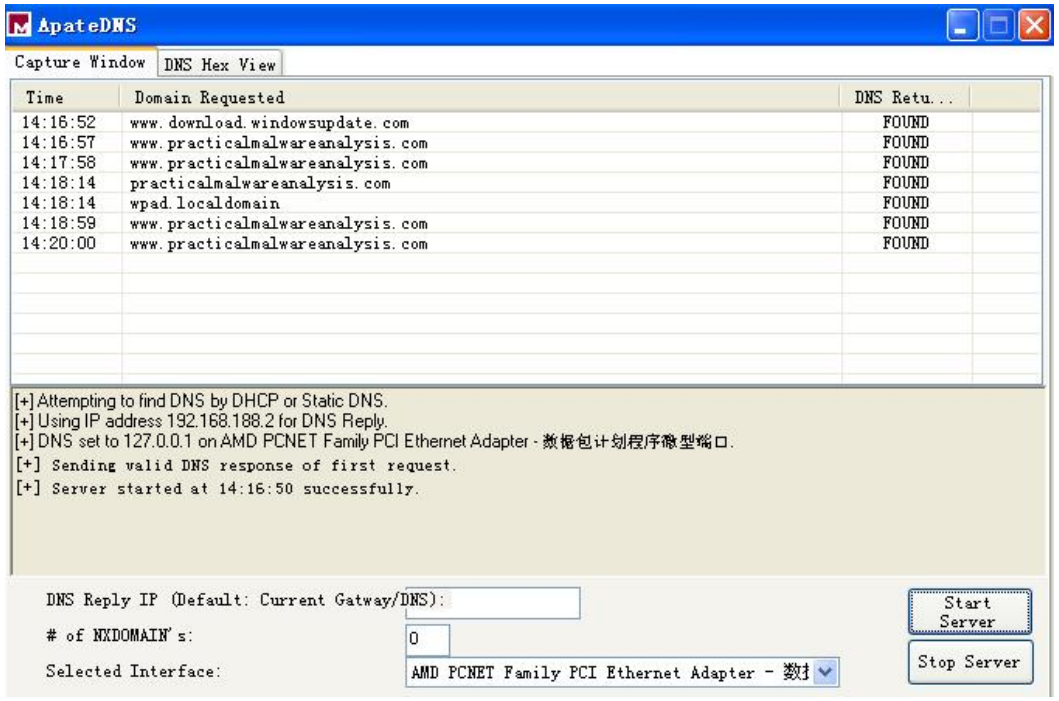
Lab2 网络分析

ApateDNS

恶意代码向practicalmabwareanalysis.com发送了DNS请求

Netcat

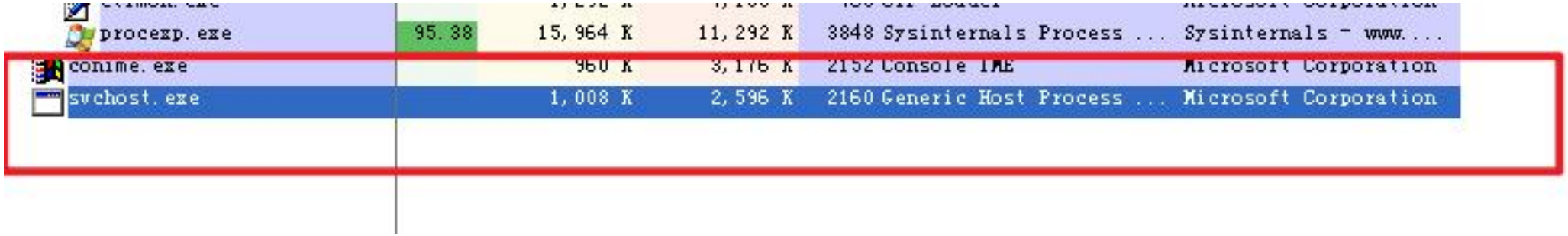
恶意代码执行了一个通过80端口的HTTP GET请求



Lab3 运行恶意代码

运行恶意代码文件，在Process Explorer中可以看到Lab03-03.exe

它还创建了子进程svchost.exe，创建之后就退出了，Scvhost.exe进程继续作为一个孤儿进程执行



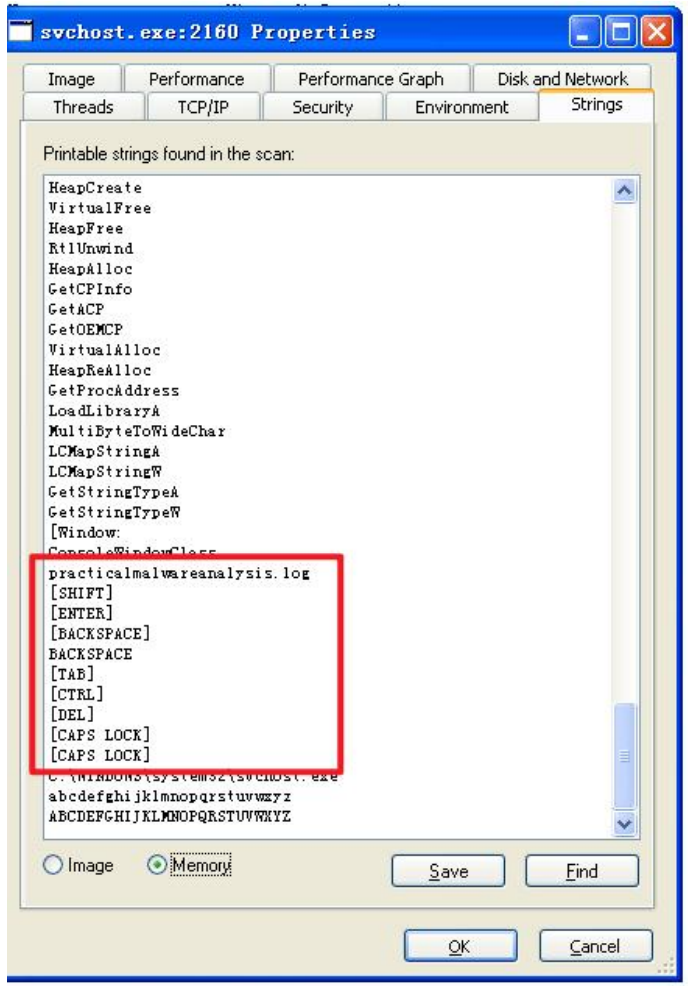
procexp.exe	95.38	15,964 K	11,292 K	3848 Sysinternals Process ...	Sysinternals - www....
conime.exe		960 K	3,176 K	2152 Console IME	Microsoft Corporation
svchost.exe		1,008 K	2,596 K	2160 Generic Host Process ...	Microsoft Corporation

这个进程看起来像是一个合法svchost.exe进程

但这个svchost.exe是很可疑的，因为svchast.exe通常是services.exe的子进程

Lab3 svchost.exe进程

选择该进程，右击选择Properties，选择Strings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

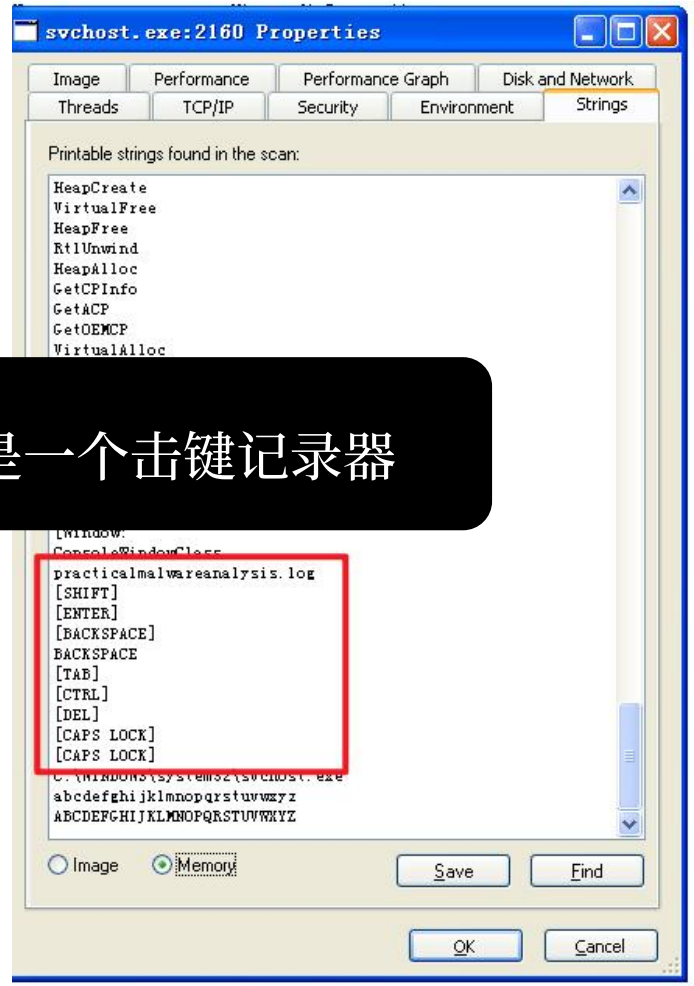


Lab3 svchost.exe进程

内存镜像中的字符串列表里包含了practicalmalwareanalysis.log和[ENTER]

而它们都不会在磁盘镜像中一个典型的svchost.exe文件中出现

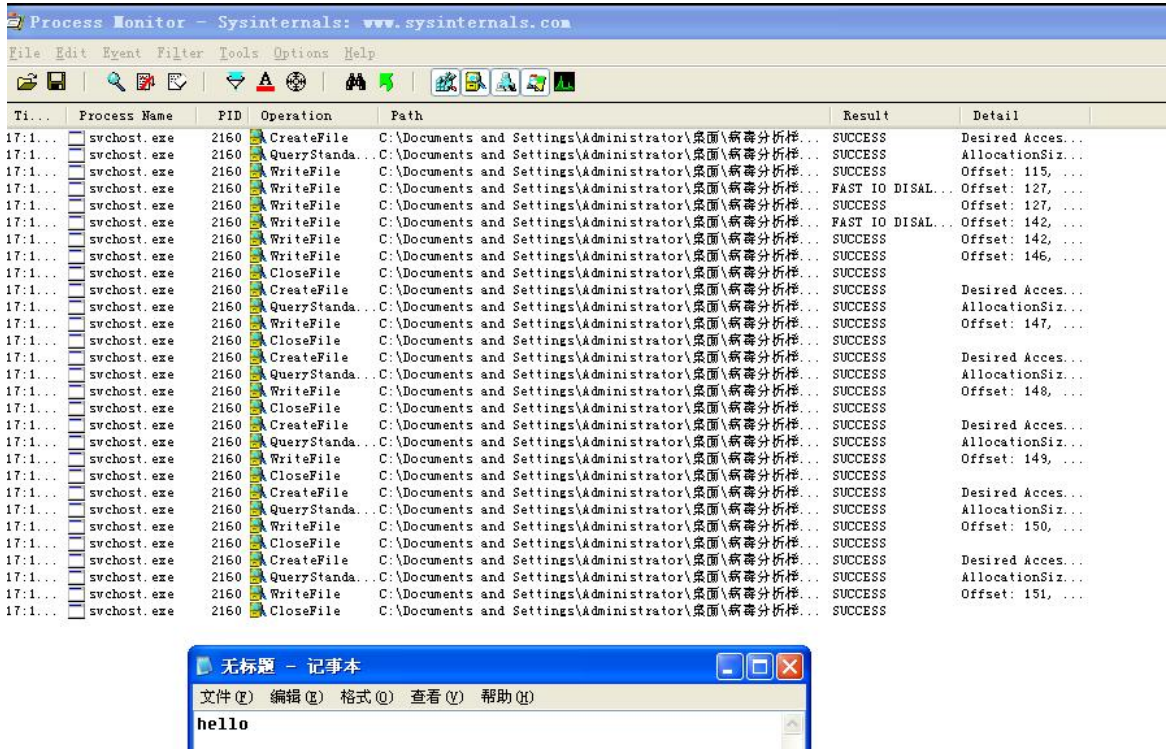
这个程序很可能是一个击键记录器



Lab3 Process Monitor

- 使用swchost.exe的PID创建一个过滤器
- 打开记事本程序，键入信息

可以发现，svchost.exe的CreateFile和WriteFile事件正在写一个名为practicalmalwareanalysis.log的文件



Lab3 Process Monitor

打开日志文件，可以发现刚刚的击键记录被记录：

可以发现，svchost.exe的CreateFile和WriteFile事件正在写一个名为practicalmalwareanalysis.log的文件

Lab3 恶意代码的目的

打开日志文件，可以发现刚刚的击键记录被记录：

这个程序在svchost.exe进程上执行了进程替换，来启动一个**击键记录器**，将击键记录在创建的日志文件中

Lab4 静态分析

导入表

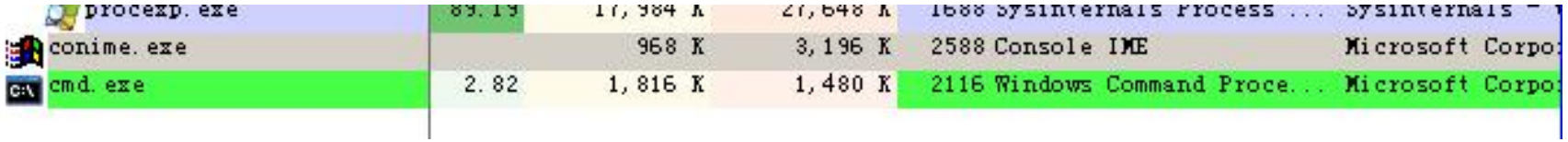
导入了一些服务操作函数、注册表操作函数、联网功能函数等

字符串

- 看到域名、注册表位置、像DOWNLOAD、UPLOAD这样的命令字符串，以及HTTP/1.0字符串等
  - 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)

Lab4 Process Explorer

启动Process Explorer，运行恶意代码



procexp.exe	89.19	17,984 K	27,648 K	1688 Sysinternals Process ...	Sysinternals -
conime.exe		968 K	3,196 K	2588 Console IME	Microsoft Corpo
cmd.exe	2.82	1,816 K	1,480 K	2116 Windows Command Proce...	Microsoft Corpo

- 可以发现，快速运行了cmd.exe，然后自行退出
- 同时发现，运行恶意代码后，恶意代码删除了自身

Lab4 Process Monitor

设置进程名称为Lab03-04.exe的过滤器，在过滤的信息中，有一个ProcessCreate的条目：

可以发现，恶意代码通过运行cmd.exe，写入命令**将自己删除**

Lab4 Process Monitor

可以发现，恶意代码通过运行cmd.exe，写入命令**将自己删除**

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

尝试使用命令行运行恶意代码，并使用在字符串列表中发现的一些命令行参数(-in、-re、-cc)，但都以失败告终，结果程序还是会删除自身

```
C:\Documents and Settings\Administrator\桌面\Practical Malware Analysis Labs\Bin
aryCollection\Chapter_3L>Lab03-04.exe -in

C:\Documents and Settings\Administrator\桌面\Practical Malware Analysis Labs\Bin
```

Lab5 Yara

```
rule Lab03_01 {
    meta:
        description = "Lab03-01.exe"
    strings:
        $s1 = "vmx32to64.exe" fullword ascii
        $s2 = "SOFTWARE\\Classes\\http\\shell\\open\\commandV" fullword ascii
        $s3 = " www.practicalmalwareanalysis.com" fullword ascii
        $s4 = "advpack" fullword ascii
        $s5 = "VideoDriver" fullword ascii
        $s6 = "WinVMX32-" fullword ascii
        $s7 = "Software\\Microsoft\\Active Setup\\Installed Components\\" fullword ascii
    condition:
        uint16(0) == 0x5a4d and
        uint32(uint32(0x3c))==0x00004550 and filesize < 20KB and
        5 of them
}
```

Lab5 Yara

```
rule Lab03_02 {
    meta:
        description = "Lab03-02.dll"
    strings:
        $x1 = "%SystemRoot%\\System32\\svchost.exe -k " fullword ascii
        $s3 = "RegOpenKeyEx(%s) KEY_QUERY_VALUE error ." fullword ascii
        $s4 = "practicalmalwareanalysis.com" fullword ascii
        $s5 = "Lab03-02.dll" fullword ascii
        $s6 = "RegOpenKeyEx(%s) KEY_QUERY_VALUE success." fullword ascii
        $s7 = "serve.html" fullword ascii
        $s8 = "GetModuleFileName() get dll path" fullword ascii
        $s9 = "netsvcs" fullword ascii
        $s10 = "OpenService(%s) error 2" fullword ascii
        $s11 = "OpenService(%s) error 1" fullword ascii
        $s12 = "CreateService(%s) error %d" fullword ascii
        $s13 = "You specify service name not in Svchost//netsvcs, must be one of following:" fullword ascii
        $s14 = "RegQueryValueEx" fullword ascii
        $s15 = "Depends INA+" fullword nocase
    condition:
        uint16(0) == 0x5a4d and
        uint32(uint32(0x3c))==0x00004550 and filesize < 70KB and
        all of ($x*) and 6 of them
}
```

Lab5 Yara

```
rule Lab03_03 {
    meta:
        description = "Lab03-03.exe"
    strings:
        $s1 = "\\svchost.exe" fullword ascii
        $s2 = "+A+A+A+A" fullword ascii
    condition:
        uint16(0) == 0x5a4d and
        uint32(uint32(0x3c))==0x00004550 and filesize < 200KB and
        all of them
}
```

Lab5 Yara

```
rule Lab03_04 {
    meta:
        description = "Lab03-04.exe"
    strings:
        $s1 = "http://www.practicalmalwareanalysis.com" fullword ascii
        $s2 = "%SYSTEMROOT%\\system32\\" fullword ascii
        $s3 = " HTTP/1.0" fullword ascii
        $s4 = " Manager Service" fullword ascii
        $s5 = "UPLOAD" fullword ascii
        $s6 = "DOWNLOAD" fullword ascii
        $s7 = "command.com" fullword ascii
        $s8 = "COMSPEC" fullword ascii
        $s9 = "SOFTWARE\\Microsoft \\XPS" fullword ascii
        $s10 = "/c del " fullword ascii
        $s11 = " >> NUL" fullword ascii
    condition:
        uint16(0) == 0x5a4d and
        uint32(uint32(0x3c))==0x00004550 and filesize < 200KB and
        8 of them
}
```

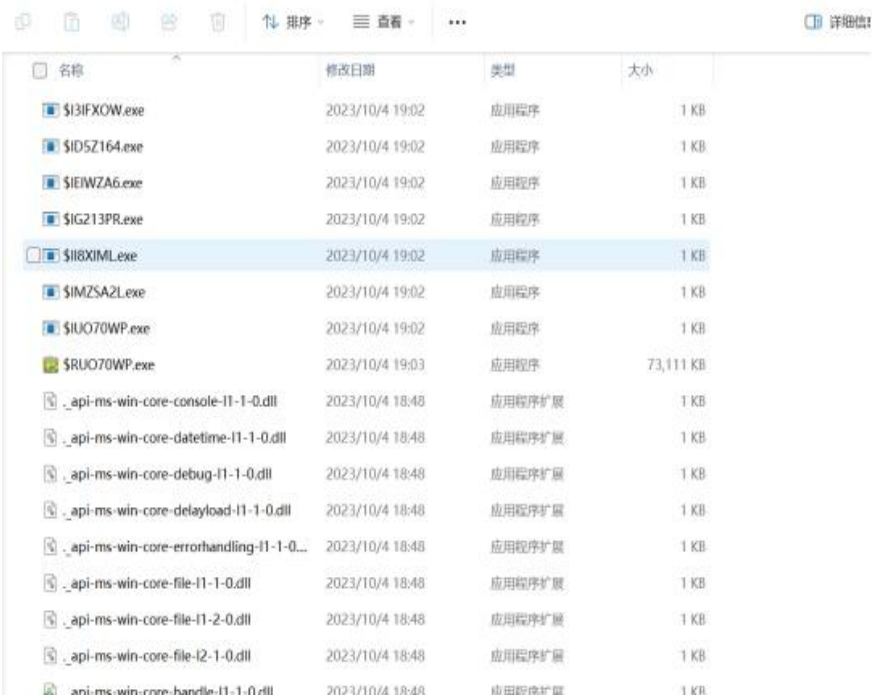
Lab5 Yara

运行yara规则，能够扫描到对应的恶意代码文件：

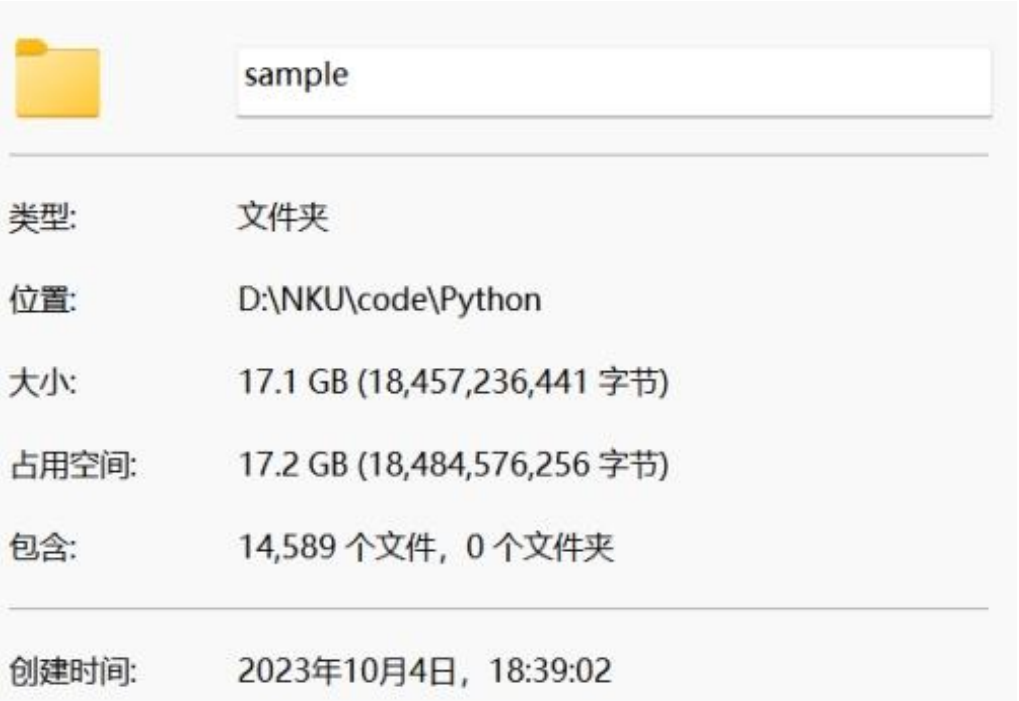
```
C:\Documents and Settings\Administrator\桌面\yara-v2.0.0-win32>yara32 lab03.yar
Chapter_3L
Lab03_01 Chapter_3L\Lab03-01.exe
Lab03_02 Chapter_3L\Lab03-02.dll
Lab03_03 Chapter_3L\Lab03-03.exe
Lab03_04 Chapter_3L\Lab03-04.exe
```

Lab5 Yara

利用scan.py程序，自动收集电脑上的所有PE结构文件，文件保存到sample文件夹中



名称	修改日期	类型	大小
$I3IFXOW.exe	2023/10/4 19:02	应用程序	1 KB
$ID5Z164.exe	2023/10/4 19:02	应用程序	1 KB
$IEIWZA6.exe	2023/10/4 19:02	应用程序	1 KB
$IG213PR.exe	2023/10/4 19:02	应用程序	1 KB
$II8XIML.exe	2023/10/4 19:02	应用程序	1 KB
$IMZSA2L.exe	2023/10/4 19:02	应用程序	1 KB
$IUO70WP.exe	2023/10/4 19:02	应用程序	1 KB
$RUO70WP.exe	2023/10/4 19:03	应用程序	73,111 KB
_api-ms-win-core-console-l1-1-0.dll	2023/10/4 18:48	应用程序扩展	1 KB
_api-ms-win-core-datetime-l1-1-0.dll	2023/10/4 18:48	应用程序扩展	1 KB
_api-ms-win-core-debug-l1-1-0.dll	2023/10/4 18:48	应用程序扩展	1 KB
_api-ms-win-core-delayload-l1-1-0.dll	2023/10/4 18:48	应用程序扩展	1 KB
_api-ms-win-core-errorhandling-l1-1-0...	2023/10/4 18:48	应用程序扩展	1 KB
_api-ms-win-core-file-l1-1-0.dll	2023/10/4 18:48	应用程序扩展	1 KB
_api-ms-win-core-file-l1-2-0.dll	2023/10/4 18:48	应用程序扩展	1 KB
_api-ms-win-core-file-l2-1-0.dll	2023/10/4 18:48	应用程序扩展	1 KB



Lab5 Yara

编写c++程序，对sample文件夹进行扫描，并得到扫描时间

```cpp
#include <iostream>
#include <windows.h>
#include <string>
using namespace std;

string cmdPopen(const string& cmdLine) {
    char buffer[1024] = { '\0' };
    FILE* pf = NULL;
    pf = _popen(cmdLine.c_str(), "r");
    if (NULL == pf) {
        printf("Open pipe failed\n");
        return string("");
    }
    string ret;
    while (fgets(buffer, sizeof(buffer), pf)) {
        ret += buffer;
    }
    _pclose(pf);
    return ret;
}

int main() {
    // 设置工作目录
    wstring workingDir = L"D:\\NKU\\23Fall\\yara-master-1798-win64";
    if (!SetCurrentDirectory(workingDir.c_str())) {
        cout << "Failed to set the working directory" << endl;
        return 1;
    }

    long long start, end, freq;
    string cmdLine = " .\\yara64 -r lab03.yar D:\\NKU\\code\\Python\\sample"; // 执行的指令

    QueryPerformanceFrequency((LARGE_INTEGER*)&freq);
    QueryPerformanceCounter((LARGE_INTEGER*)&start);
    string res = cmdPopen(cmdLine);
    QueryPerformanceCounter((LARGE_INTEGER*)&end);
    cout << "扫描到的文件: " << endl;
    cout << res; // 输出 cmd 指令的返回值
    cout << "运行时间为 " << (end - start) / freq << "s" << endl;
    return 0;
}
```

Microsoft Visual Studio 调试控

```
扫描到的文件:
Lab03_01 D:\NKU\code\Python\sample\Lab03-01.exe
Lab03_02 D:\NKU\code\Python\sample\Lab03-02.dll
Lab03_04 D:\NKU\code\Python\sample\Lab03-04.exe
Lab03_03 D:\NKU\code\Python\sample\Lab03-03.exe
Lab03_04 D:\NKU\code\Python\sample\Lab09-01.exe
Lab03_04 D:\NKU\code\Python\sample\Lab16-01.exe
运行时间为 9s
```

Summary

- 本次实验综合使用静态分析技术和动态分析技术分析恶意代码；
- 熟练了基本静态分析和动态分析工具的使用，掌握了基本分析方法；
- 练习和熟练了Yara规则的编写。

THANK YOU!