Practical Malware Analysis Lab 3-1

Questions

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

Question 1

When putting the exe Lab03-01.exe into Dependencies it only showed one import kernel32.dll and the function ExitProcess. The strings gave us more information about what this malware does.

StubPath

Software\Microsoft\Active Setup\Installed Components\

test

www.practicalmalwareanalysis.com

Admin

?503

200

advpack

CONNECT %s:%i HTTP/1.0

VideoDriver

WinVMX32-

Vmx32to64.exe

Software\Microsoft\Active Setup\Installed Components\

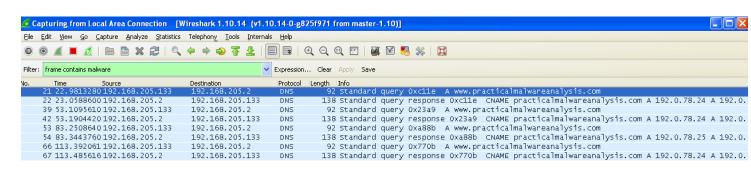
 $SOFTWARE \backslash Microsoft \backslash Windows \backslash Current Version \backslash Run$

Dynamic Analysis

Regshot Results

```
| Stream No. | No.
```

Wireshark Results



Process Monitor Results

```
1:54:2... Lab03-01.exe
1:54:2... Lab03-01.exe
1:54:2... Lab03-01.exe
                                2040 🌋 RegSetValue
                                                           HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS
                                                                                                                          Type: REG_BINA...
                                2040 RegSetValue
2040 RegSetValue
2040 RegSetValue
                                                           HKLM\SOFTWARE\Microsoft\Window... SUCCESS
                                                                                                                          Type: REG_SZ, Le..
                                                                                                                          Type: REG_BINA..
                                                           HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS
         Lab03-01.exe
                                                                                                                          Type: REG_BINA Type: REG_SZ
Type: REG_BINA Length: 510
1:54:2...
                                                           HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS
         ____Lab03-01.exe
1:54:2...
                                2040 MRegSetValue
                                                           HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS
1:54:2... Lab03-01.exe
                                                                                                                          Type: REG_BINA Data: C:\WINDOWS\system32\vmx32to6
                                2040 KRegSetValue
                                                           HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS
                                2040 RegSetValue
2040 RegSetValue
2040 RegSetValue
1:54:2... Lab03-01.exe
1:54:2... Lab03-01.exe
                                                           HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS
                                                                                                                          Type: REG_BINAT
                                                                                                                          Type: REG_BINA.
                                                           HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS
1:54:2... Lab03-01.exe
                                                           HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS
                                                                                                                          Type: REG_BINA.
```

Question 2

Some host based indicators include the exe C:\Windows\system32\Vmx32to64.exe , and the registry entry of VideoDriver.

Question 3

Traffic to the website www.practicalmalwareanalysis.com