

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\Classes\http\shell\open\commandV

Software\Microsoft\Active Setup\Installed Components\

test

www.practicalmalwareanalysis.com

Admin

?503

200

advpack

CONNECT %s:%i HTTP/1.0

VideoDriver

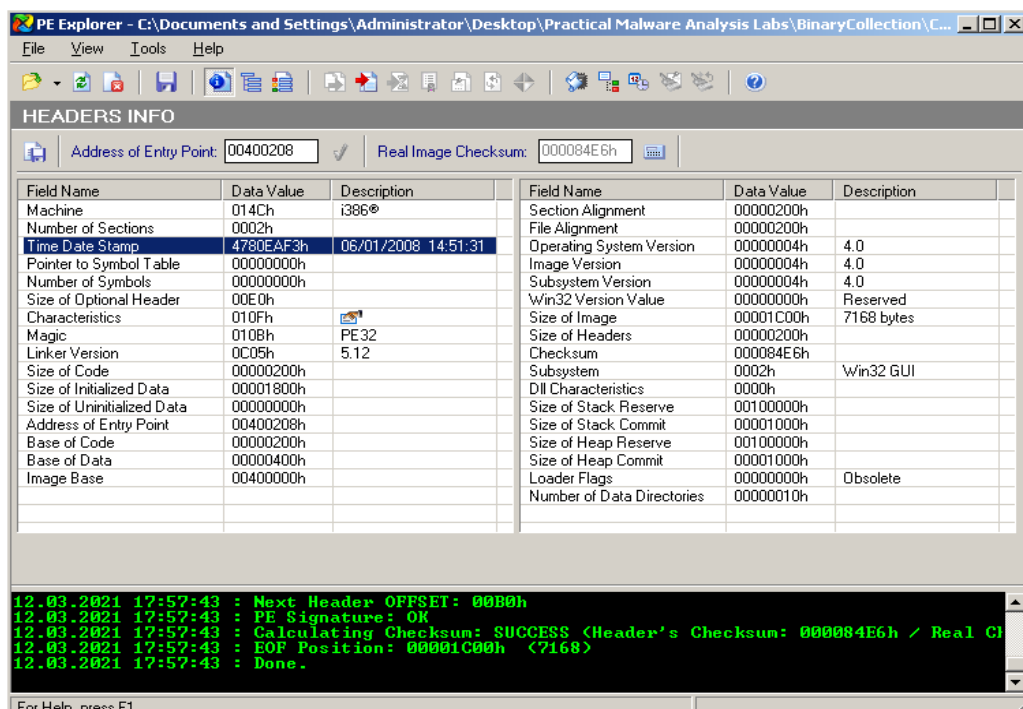
WinVMX32-

Vmx32to64.exe

SOFTWARE\Classes\http\shell\open\commandV

Software\Microsoft\Active Setup\Installed Components\

SOFTWARE\Microsoft\Windows\CurrentVersion\Run



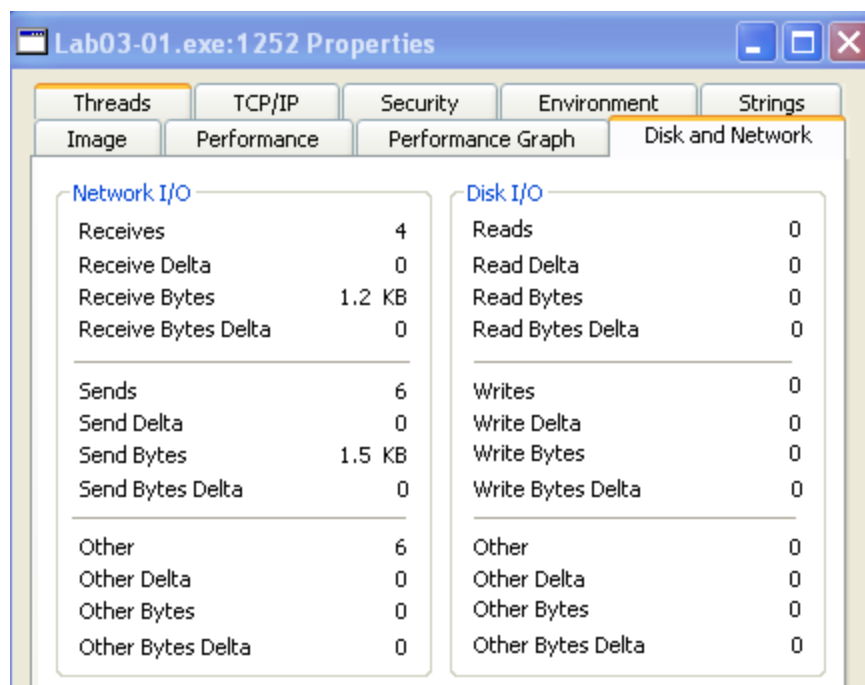
Dynamic Analysis

Regshot Results

```
-res-x86 - Notepad
File Edit Format View Help
HKU\S-1-5-21-2000478354-113007714-682003330-500\Software\Microsoft\Advanced INF Setup\IEHomePageInfo\RegBackup\0.map\3bdd6b017b35029e: ",1,HKCU,Software\Microsoft\Inter
-----
values added: 203
-----
HKLM\SOFTWARE\Classes\.svw\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.acp\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.apc\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.atc\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.bfr\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.cap\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.enc\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.erf\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.fdc\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.ntar\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.out\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.pcap\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.pcapng\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.pkt\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.rf5\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.snop\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.sys\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.tpc\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.trf\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.trace\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.trc\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.vmr\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.wpc\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\.wpz\:"wireshark-capture-file"
HKLM\SOFTWARE\Classes\wireshark-capture-file\:"wireshark capture file"
HKLM\SOFTWARE\Classes\wireshark-capture-file\DefaultIcon\:"C:\Program Files\wireshark\wireshark.exe",1"
HKLM\SOFTWARE\Classes\wireshark-capture-file\Shell\open\command\:"C:\Program Files\wireshark\wireshark.exe" "%1"
HKLM\SOFTWARE\Microsoft\ESent\Process\wireshark\DEBUG\Trace Level\:""
HKLM\SOFTWARE\Microsoft\WBEM\CIMOM\ADAPPerf1btTimeout\:"0x0000003C"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\wireshark.exe\:"C:\Program Files\wireshark\wireshark.exe"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\wireshark.exe\Path\:"C:\Program Files\wireshark"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\DisplayName\:"WinPcap 4.1.3"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\UninstallString\:"C:\Program Files\WinPcap\uninstall.exe"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\Publisher\:"Riverbed Technology, Inc."
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\URLInfoAbout\:"http://www.riverbed.com/"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\URLUpdateInfo\:"http://www.winpcap.org"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\VersionMajor\:"4"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\VersionMinor\:"1"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\DisplayVersion\:"4.1.0.2980"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst\DisplayIcon\:"C:\Program Files\WinPcap\uninstall.exe"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark\Comments\:"Wireshark 1.10.14 (32-bit)"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark\DisplayIcon\:"C:\Program Files\wireshark\wireshark.exe,0"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark\DisplayName\:"Wireshark 1.10.14 (32-bit)"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark\DisplayVersion\:"1.10.14"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark\HelpLink\:"http://ask.wireshark.org/"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark\InstallLocation\:"C:\Program Files\Wireshark"
```

Wireshark Results

Capturing from Local Area Connection [Wireshark 1.10.14 (v1.10.14-0-g825f971 from master-1.10)]									
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help									
Filter: frame contains malware Expression... Clear Apply Save									
No.	Time	Source	Destination	Protocol	Length	Info			
21	22.9813280	192.168.205.133	192.168.205.2	DNS	92	Standard	query 0xc11e	A	www.practicalmalwareanalysis.com
22	23.0588600	192.168.205.2	192.168.205.133	DNS	138	Standard	query response 0xc11e	CNAME	practicalmalwareanalysis.
39	53.1095610	192.168.205.133	192.168.205.2	DNS	92	Standard	query 0x23a9	A	www.practicalmalwareanalysis.com
42	53.1904420	192.168.205.2	192.168.205.133	DNS	138	Standard	query response 0x23a9	CNAME	practicalmalwareanalysis.
53	83.2508640	192.168.205.133	192.168.205.2	DNS	92	Standard	query 0xa88b	A	www.practicalmalwareanalysis.com
54	83.3443760	192.168.205.2	192.168.205.133	DNS	138	Standard	query response 0xa88b	CNAME	practicalmalwareanalysis.
66	113.392061	192.168.205.133	192.168.205.2	DNS	92	Standard	query 0x770b	A	www.practicalmalwareanalysis.com
67	113.485616	192.168.205.2	192.168.205.133	DNS	138	Standard	query response 0x770b	CNAME	practicalmalwareanalysis.



Question 2

Some host based indicators include the exe Vmx32to64.exe, and the registry entry of VideoDriver.

Question 3

Traffic to the website www.practicalmalwareanalysis.com