Practical Malware Analysis Lab 1-1

Questions

1. Upload the files to http://www.VirusTotal.com/ and view the reports. Does either file match any existing antivirus signatures?
2. When were these files compiled?
3. Are there any indications that either of these files is packed or obfuscated? If so, what are these indicators.?
4. Do any imports hint at what this malware does? If so, which imports are they?
5. Are there any other files or host-based indications you could look for on infected systems?
6. What network-based indicators could be used to find this malware on infected machines?
7. What would you guess is the purpose of these files.

Question 1

Result of Lab01-01.dll
Md5: 290934c61de9176ad682ffdd65f0a669
Result of Lab01-01.exe
Md5: bb7425b82141a1c0f7d60e5106676bb1

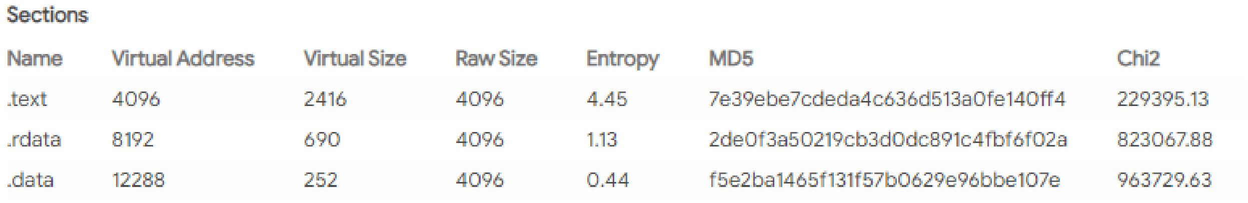
Both these files seem fairly malicious! The DLL was detected by 40/68 engines and the EXE was detected out of 49/68 engines. The word Trojan keeps popping up within these 2 reports.

Question 2

According to the VT (virus total) report the EXE was compiled on 2010-12-19 16:16:19 and the DLL was compiled on 2010-12-19 16:16:38.

Question 3

I don't believe this malware is packed. The virtual size is lower then the raw size and various imports are shown which leads me to the conclusion that this file is also not obfuscated.



Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	2416	4096	4.45	7e39ebe7cdeda4c636d513a0fe140ff4	229395.13
.rdata	8192	690	4096	1.13	2de0f3a50219cb3d0dc891c4fbf6f02a	823067.88
.data	12288	252	4096	0.44	f5e2ba1465f131f57b0629e96bbe107e	963729.63

Question 4

The EXE imports two libraries kernel32.dll and MSVCRT.dll.

Kernal32.dll

- CloseHandle
- UnmapViewOfFile
- IsBadReadPtr
- MapViewOfFile
- CreateFileMappingA
- CreateFileA
- FindClose
- FindNextFileA
- FindFirstFileA
- CopyFileA

MSVCRT.dll

- Malloc
- Exit
- _XcptFilter
- __p__initenv
- __getmainargs
- _initterm
- _setusermatherr
- _adjust_fdiv
- __p__commode
- __p__fmode
- __set_app_type
- __except_handler3
- _controlfp
- _stricmp

The DLL imports three libraries kernel32.dll, WS2_32.dll and MSVCRT.dll.

- **Kernel32.dll**
  - Sleep
  - CreateProccessA
  - CreateMuteXA
  - OpenMutexA
  - CloseHandle
- **WS2_32.dll**
  - Dependencies couldnt display imports despite changing the Tree build behavior.

However this DLL handles sockets.

MSVCRT.dll

_adjust_fdiv
Malloc
_initterm
Free
Strncmp

The EXE seems to handle files while the DLL works with processes and sockets; this could possibly be a backdoor. When running the command strings on the DLL it displays an IP address: 127.26.152.13. When using the same command on the exe it displays:

```
kerne132.dll
kernel32.dll
C:\*
C:\windows\system32\kerne132.dll
Kernel32.
Lab01-01.dll
C:\Windows\System32\Kernel32.dll
WARNING_THIS_WILL_DESTROY_YOUR_MACHINE
```

Maybe the EXE drops the Fake dll c

Question 5

The EXE imported various modules involving file creation. I would watch for new files popping up such as kerne132.dll.

Question 6

Check for a connection to the ip: 127.26.152.13

Question 7

I think this malware creates a new dll kerne132.dll and Lab01-01.dll and creates a backdoor to the ip address 127.26.152.13.