Practical Malware Analysis Lab 1-2

Questions

1. Upload the Lab01-02.exe file to https://www.VirusTotal.com/. Does it match any existing antivirus definitions?
2. Are there any indications that this file is packed or obfuscated? If so, what are these indications? If the file is packed, unpack it if possible.
3. Do any imports hint at this program's functionality? If so, which imports are they and what do they tell you?
4. What host- or network-based indicators could be used to identify this malware on infected machines?

Question 1

Report for Lab-1-02.exe
MD5: 8363436878404da0ae3e46991e355b83

This EXE definitely seems malicious. The file was detected by 53/68 engines.

Question 2

I believe this file is packed. The virtual size is much higher than it should be for a non packed file. Also VirusTotal says it was packed with UPX v0.89 to v1.02 / v.1.05-v.1.24. I don't believe this file is obfuscated however various imports are show.

Sections

Name	Virtual Address	Virtual Size	MD5	Chi2
UPX0	4096	16384	d41d8cd98f00b204e9800998ecf8427e	-1
UPX1	20480	4096	ad0f236c2b34f1031486c8cc4803a908	5848.3
UPX2	24576	4096	f998d25f473e69cc89bf43af3102beea	53922

File size	3.00 KB (3072 bytes)
PEiD packer	UPX v0.89.6 - v1.02 / v1.05 -v1.24 -> Markus & Laszlo [overlay]
F-PROT packer	UPX

```
drew@ubuntu:~$ upx -d Lab01-02.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2018
UPX 3.95        Markus Oberhumer, Laszlo Molnar & John Reiser   Aug 26th 2018

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
```

16384 <- 3072 18.75% win32/pe Lab01-02.exe

Unpacked 1 file.

Question 3

Lab-1-0-2.exe imports 3 dlls kernel32.dll, advapi32.dll, MSVCRT.dll and WININET.dll

Kernel32.dll

- **LoadLibraryA**
- **GetProcAddress**
- SetWaitableTimer
- VirutalProtect
- VirualAlloc
- VirtualFree
- WaitForSingleObject
- ExitProccess

Advapi.dll

- **CreateServiceA**

MSVCRT.dll

- exit

WININET.dll

- **InternetOpenA**
- **InternetOpenUrlA**

Using the command strings on this malware sample results in:
InternetOpenUrlA
InternetOpenA
MalService
Malservice
HGL345
http://www.malwareanalysisbook.com
Internet Explorer 8.0

Maybe this malware connects the url “http://www.malwareanalysisbook.com”. The function InternetOpenA initializes the user agent in the HTTP protocol. And InternetOpenURL which connects to the actual url. Some modules mention time such as SetWaitableTimer and WaitForSingleObject maybe this is a logic bomb. Also a service called MalServices is mentioned (CreateServiceA).

Question 4

Watch for traffic to the url http://www.malwareanalysisbook.com and the service Malservice.