Muhammad Izham Bin Norhamadi  
B032020039

# Lab 4 Basic Static Malware Analysis

Task 1

**1)** Yes, it has similarities with other sandbox test virus.

Lab01-01.exe

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Lab01-01.dll

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

**2)**

Lab01-01.exe

2010-12-19 16:16:19

Lab01-01.dll

2010-12-19 16:16:38

**3)** None of the files is packed or obfuscated, since all the PE sections have much larger raw sizes than virtual sizes.

Lab01-01.exe

Graphical user interface, application

Description automatically generated

Lab01-01.dll

Table

Description automatically generated

**4)** Imports:

Kernel32.dll

* Is a Windows kernel module
* Runs as a background process and carries out important functions like memory management, input/output operations and interrupts
* The malware will search through file system

MSVCRT.dll

* is the C standard library for the Visual C++
* provides programs with standart C functions such as string manipulation, memory allocation, C-style input/output calls, and others

WS2\_32.dll

* establish and handle network connections
* contains the Windows Sockets API
* used to run most network and internet applications

**5)**

**Graphical user interface

Description automatically generated**

Dissambling lab01-01.exe will find strings around kernel32.dll

**6)**

Graphical user interface

Description automatically generated

An IP 127.26.152.13 was found with other strings after disassembling Lab01-01.dll

**7)**

Lab01-01.exe and Lab01-01.dll are likely related and functions together to search through directories on the infected system. The presence of IP address and network based imports can be used to send information.

Task 2

**1)**

Graphical user interface, text, application

Description automatically generated

53 out of 68 antivirus detected this exe as malicious with most of them detect it as a Trojan.

**2)** Yes, the file is packed. The virtual size of the sections are much bigger than the raw size. The packer that was used is UPX packer. Unpacked using PE explorer

A screenshot of a computer

Description automatically generated with medium confidence

UPX Unpacker plugin unpacked the exe

**3)** The imports are ADVAPI32.dll, KERNEL32.DLL, MSVCRT.dll, WININET.dll. Noteable services are CreateServiceA and InternetOpenA

**4)**

Graphical user interface

Description automatically generated

After disassembling the exe, in the strings of the file contains the link to malwareanalysisbook.com and Internet Explorer 8.0 that potentionally act as a host or network based indicators of malicious activity, through the service to run, URL to connect to and preferred browser.

Task 3

1)

Graphical user interface, text, application

Description automatically generated

57 out of 66 antivirus detected this exe as malicious with most of them detect the exe as Trojan or Spyware.

2)

Yes, the file is packed with the packer FSG v1.00 (Eng) -> dulek/xt. Unable to unpack the file with PE Explorer plugins

A screenshot of a computer

Description automatically generated with medium confidence

3)

The import doesn’t tell much, just KERNEL32.dll which is imported by most programs for creating process.

4)

Text

Description automatically generated

Unprocessed data doesn’t give much hint on the malware.