LAB

4

Basic Static Malware Analysis

By the end of this section of the practical, you should be able to:

- Understand the basics techniques of static malware analysis
- Used the basic tool to perform a basic static analysis
- Interpret the output of basic static analysis

Introduction

Static Malware analysis is a process of analysing the code or structure of a program without having to run the program in real time. The aim of the analysis is to determine its function and behaviour through the code. The advantage of a static analysis is that we can reveal how a program would behave under unusual conditions, because we can examine parts of a program that normally do not execute.

However the drawback of the static analysis is that it is tedious process and it is impossible to fully predict the behaviour due to obfuscation. Among The basic technique used in this analysis are:

- Using antivirus tools to confirm maliciousness
- Using hashes to identify malware
- Gleaning information from a file’s strings, functions, and headers

Each technique can provide different information, and the ones you use depend on your goals.

Some basic tools to perform these techniques are:-

1. http://www.VirusTotal.com/
2. HashCalculator
3. BinText
4. Hex Editor
5. PEiD

Task 1

http://www.Virustotal.com

This lab uses the files Lab01-01.exe and Lab01-01.dll. Use the tools and techniques described in the chapter to gain information about the files and answer the questions below.

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 indicators that 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?

Task 2

Analyse the file Lab01-02.exe.

Questions

1. Upload the Lab01-02.exe file to http://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 indicators? 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?

Task 3

Analyse the file Lab01-03.exe.

Questions

1. Upload the Lab01-03.exe file to http://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 indicators? 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?