Information systems security
Malware analysis

The trend of increasing criminal activities on the Internet has been noticeable for several years. Namely, the number of malicious programs that are being developed in a targeted manner for the purpose of stealing the data of Internet users is on a significant increase and certainly calls for caution.

The goal of this laboratory exercise is to acquaint students with the basics of analyzing malicious programs.

Tools used in this lab exercise:

- **HxD – Hex Editor**
  - The tool is used to analyze binary files
- **JD-Gui**
  - Java decompiler
  - A tool for analyzing the source code of java applications

NOTE: Everything needed for this exercise can be found at the following link: https://tinyurl.com/5dpvcax2.

Download the Malware_LAB_2.rar file to a Windows virtual machine (Hyper-V). Download and install winrar or 7-zip from the Internet in order to unpack the compressed file. The password is "infected".

1. Install the necessary tools found in the tools directory

Install:

- jd-gui-0.3.2.windows.zip
- HxDSetupEN.zip
- Download strings tool from Microsoft site

2. JAR file analysis

The Dynamite.jar file is a time bomb simulator. Your task is to find out the time when the bomb is activated. Try to "crack" the hash with online tools or use the python script included in the task. If you use a python script, you also need a python installation.

Using strings and the HxD tool, analyze the contents of the file.

Using the JD-Gui tool, decompile the file and analyze the program code.

In what form is the bomb activation time stored? ______________________

In what time units is time calculated? _______________________

Which hash algorithm is used? _______________________

Identify the digest of the explosion and write it in the appropriate field of the md5_bf.py script or use google to identify the hashed value.

What is the activation time of the "bomb" in seconds? ___________________

What is the activation time in HH:MM:SS format? _____________________