Lab 2. Malware creation

Compilable programming languages shall be used, like: C, C++, Rust, C# (only for Windows OS), Go, D, etc. Also, scripting languages, like: PowerShell, Bash, Batch, can be used.

The malware should implement the following:

1. Obfuscation

- C++ String and code obfuscator;
- Rust obfuscator;
- C# Obfuscator.

2. System persistence

Collection of malware persistence information

3. Controlled environment detection

Here you have a list of ways to detect if you run in a controlled environment (for analyzing malware) or a real system. Try to implement some of them by yourself.

4. Communication with command and control server

Here you can find inspiration for your OWN server. It can be written in any language you like.

5. Detection evasion techniques

RedTeaming-Tactics-and-Techniques repository contains a collection of red teaming and pentesting notes, experiments, and techniques for offensive security.