BINARY

Professionals from Binary House are ready to assist you in analysing a malicious code, a binary/executable file by reverse engineering or writing a PoC/exploit.

MALICIOUS CODE ANALYSIS

If your organization has been infected with a malicious code, this service will help you get detailed information about its functionality and the risk it represents for your organisation. Typical malicious code is found in various scripts, mobile applications, documents and executable files.

The output is a detailed report with the results of the analysis and a list of recommendations to respond to a similar type of attack.

REVERSE ENGINEERING

Reverse engineering (RE) is the process of retrieving information from supplied files. This service will help you especially in the following cases:

- Understanding proprietary network protocol and file formats
- Identification of changes in a system or an application made by patching
- Rebuilding part of the functionality of an executable file due to lost source code.

During the project we use static and dynamic analysis to get information about the functionality of a executable file or its part. We understand the following architectures:

- x86
- x86-64
- ARM
- ARM64
- MIPS

Upon completion of the analysis, you will receive a detailed report with the required information.

EXPLOIT DEVELOPMENT

In penetration tests or in verification if a vulnerability has been fixed, it is sometimes necessary to use an exploit or "proof of concept" (PoC). As exploits/PoC are usually not publicly available, we can therefore develop them for customer needs.