# Web Security and Malware Analysis

## Assignment 8 – 03/05/2021

**Goal:** Solve each task by providing a brief explanation of the solution that you adopted. Answers should mainly include screenshots and some brief comments. Use the provided template to write your assignment.

**What to do:** Save the Assignment as a PDF and submit it to the E-Learning platform (**Section: Assignment 8**). The file should be named as follows: **"websec_report_8_name_surname.pdf".** Remember to include your name, surname, and matriculation number in your report.

**Starting Notes:** Please remember that the files you are going to deal with are real malicious samples, which could potentially destroy your machine. DO NOT EXECUTE OR OPEN THEM in your own system. ALWAYS USE A VIRTUAL MACHINE (VMware/VirtualBox) FOR EVERY OPERATION. Save a snapshot. Additionally, you could execute the tools in a virtualized environment with the Sandboxie tool (https://www.sandboxie.com/). You can find the executables for this assignment on the e-learning platform.

(password: **malwanalysis**)

**Additional notes:** if you have problems with Windows Defender, please follow these instructions to disable it:

https://www.windowscentral.com/how-permanently-disable-windows-defender-antivirus-windows-10

If you have problems at running IDA PRO, please install Microsoft Visual C++ Redistributable Package:

https://www.microsoft.com/en-us/download/details.aspx?id=5555

To use GHIDRA, you have to install the Java JDK at the following link:https://www.oracle.com/java/technologies/javase-jdk14-downloads.html

**Task 1 – Full Malware Analysis**

You are required to perform a full malware analysis of the sample Lab09-01.exe. This will be the first open task of this part of the course (you will get another one in assignment 9 and one in the last assignment).

**Your goal is providing as much information as you can about the piece of malware you have. This malware is much more complex in comparison to what you analysed until now and hides many "secrets". Can you find them all?**

In your answer, **you must employ all the techniques learned so far, in particular**:

- Analyze the PE structure;
- Take a look at the employed strings;
- Use general static analysis with IDA/Ghidra;
- Perform dynamic analysis with off-the-shelf tools (procmon, regshot, process explorer…);
- Perform dynamic analysis with IDA (or other free debuggers as OllyDbg).

You are free to go in depth as much as you can, but be sure to motivate at least some malware behaviour by clearly showing how you obtained it.

**Remember to always take snapshots of your VM before the execution. You will most likely need to restore your VM.**

Some hints:

- The sample has some kind of "first installation" mechanism.
- The sample has an interesting way to hide itself after the execution.
- There is a special command-line "password" for this sample.
- The sample can interact with the network.

Good luck and have fun!

**Task 2 – More Static Analysis**

Given the assembly X86 code contained in the file assignment_8.txt, answer the following questions:

1. Describe what each part of the code (starting with LOC…) does. As usual, you are not required to analyze every single assembly instruction.
2. Describe the functionality of the code and write the equivalent program in C or in a pseudo-language. What does the program print?