Web Security and Malware Analysis

Assignment 9 – 17/05/2021

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 9**). The file should be named as follows: **"websec_report_9_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 Lab09-02.exe.

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.

As a general hint, this sample is easier to analyze than the one of Assignment 8 – Task 1.

Task 2 – Windows API Functionality

You are required to perform a full malware analysis of the sample Lab07-01.exe. You can either use static or dynamic analysis.

Your goal is to describe the malware behaviour by pointing out the following Windows API-related structures (if present):

- Mutex
- Threads
- Services
- Communication API

Task 3 – More Static Analysis

Given the assembly X86 code contained in the file assignment_9.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?