Web Security and Malware Analysis

Assignment 10 – 31/05/2021

Goal: Solve the final task of the course 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 10**). The file should be named as follows: **"websec_report_10_name_surname.pdf".** Remember to include your name, surname, and matriculation number in your report.

Starting Notes: Remember that the file you are analysing in this final assignment is a **real malware sample. Do not, for any reason, use your own machine to make any kind of execution. Use always a virtual machine (possibly with internet connection disconnected) or a sandbox**. Also remember to save a snapshot of the virtual machine before the execution. You can find the executable for this assignment on the Discord channel of the course.

(password: **malwanalysis**)

Final Task – Real Malware Analysis

This is the final task of the course. You are required to perform a full analysis of a real malware sample with an intermediate "destructive power". Please note that the malware name does not have an extension to avoid accidental executions. In order to execute it in your machine, you should add the extension .exe. Use all the resources and the tools you employed during the course (including sandboxes, tools, disassemblers) to analyze it. **Remember not to execute the sample, for any reason, outside**

a virtual machine. Disable the internet connection before performing any execution and disconnect all USB drives that can be connected to the machine. DO NOT EXECUTE THIS SAMPLE UNDER AN EDUROAM CONNECTION.

In the final report, you should execute a static and dynamic analysis of the sample. You will probably encounter some elements we did not fully explore during the lectures, but this is exactly due to the large variety of malware samples in the wild.

Have fun, and thank you for attending the Web Security and Malware Analysis course!