Web Security and Malware Analysis

Assignment 10 – 01-03/06/2020

Goal: Solve the final task by providing a brief explanation of the solution that you adopted. You must use IDA PRO (for disassembling/debugging) and GHIDRA (for decompiling), or one of the indicated tools to solve the tasks (when required). Explanations should mainly include screenshots and some brief comments.

Deadline: All assignments must be sent before taking the final exam.

What to do: Send the report in the PDF format to davide.maiorca@unica.it with the subject "[WEBSEC] - Report For Assignment 10 – NAME SURNAME" and name the file "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 https://gofile.io/d/gG2omN or in the Discord channel of the course.

(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

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.**

In the final report, you should provide 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!