IT Security 2024/2025

Exercise Sheet 6
– Malware Analysis –

Timo Pohl

Publication: 14.11.2024
Deadline: 20.11.2024 10:00

Lightning Survey ⚡

Exercise 1 (PDF Analysis, 0.5+0.5+0.5+1 points)**.** Consider the file `task_1.pdf` and answer the following questions. Write your answers into `pdf-analysis.yml`.

a) Which URL(s) are present in the Document?

b) Which file path(s) are present in the Document?

c) Which types of actions are used?

d) What are the ID and action type of the action that is activated when opening the PDF?

Exercise 2 (PE Analysis, 1.5+1.5+2+1+1.5 points)**.** Consider the file `task_2.exe`. Write your answers into `pe-analysis.yml`, unless specified otherwise in the subtask.

a) List the three URLs or IPs that are provided to the `login` function.

b) List the password provided to the `login` function.

c) Reimplement the decryption routine in Python and write it into a file called `decrypt.py`. It should read everything from `stdin` and output the decrypted data to `stdout` (without a trailing newline).

Additionally, answer the following questions:

d) Which anti-debugging techniques are used?

- ☐ Windows' `IsDebuggerPresent` function
- ☐ Windows' `PEB`

e) Which anti-sandboxing techniques are used? Stick to the definitions of the lecture.

- ☐ File system based
- ☐ Special CPU instructions
- ☐ Hardware detection