ADVANCED STATIC ANALYSIS

MALWARE ANALYSIS AND INCIDENT FORENSICS

M.Sc. in Cybersecurity

MALWARE ANALYSIS

M.Sc. in Engineering in Computer Science

A.Y. 2024/2025

SAPIENZA
UNIVERSITÀ DI ROMA

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

GOALS

Consider the sample provided in the 7z archive (pwd: infected)

- The sample IS NOT MALICIOUS
- You need to understand how it works
- It is a game containing a few puzzles
- You should be able to solve the puzzles

How?

- Reverse the code!

STEP 1

We first need to gather a basic understanding of the target

- Did you run it?
- How does it behave?
- Does it expect any input from the command line?
- What happens when you try to interact with it?

Outcome

- . . .
- . . .
- . . .
- . . .

STEP 2

Let’s gather some initial information using the basic tools

- Does the PE header tell you anything interesting?
- Strings?
- Imports?

Outcome

- . . .
- . . .
- . . .
- . . .

STEP 3

Open the sample in IDA and try to understand its basic structure

- Where is the main()?
- What does it tell us about the behavior of the sample?
- How is the general control flow organized in the sample?
- Do you recognize code handling any of the output you have seen?

Outcome

- . . .
- . . .
- . . .
- . . .

STEP 4

Try to overcome challenge n° 1

- Which function handles the first challenge?
- What does the function check?
- What is the expected input to pass it?

Outcome

- . . .
- . . .
- . . .
- . . .

STEP 5

Try to overcome challenge n° 2

- Which function handles the second challenge?
- How does the function handle input?
- Which kind of calculation is performed in the code?
- What is the expected input to pass it?

Outcome

- . . .
- . . .
- . . .
- . . .

STEP 6

Try to overcome challenge n° 3

- Which function handles the third challenge?
- How does the function handle input? Do you recognize any known control flow pattern?
- Which kind of checks are made on the input?
- What is the expected input to pass it?

Outcome

- . . .
- . . .
- . . .
- . . .

STEP 7

Try to overcome challenge n° 4

- Which function handles the fourth challenge?
- Why does a function call itself?
- Which kind of calculation does the function perform?
- What is the expected input to pass the challenge?

Outcome

- . . .
- . . .
- . . .
- . . .

CONCLUSION

Check the remaining challenges for further different behaviors