Reverse Engineering March, 2023

Project 0x01

Cristian Rusu

1 Problem

To test your knowledge and understanding of the subjects discussed in previous labs, you are given a considerably larger program to analyze and apply concepts of:

- black-box analysis
- white-box analysis
- gray-box analysis

The analysis of this binary imitates analyzing a real-world ransomware. A ransomware is a malicious software that seeks to encrypt files and hold them for ransom. Users must pay the hackers to regain access to files such as pictures, videos or any other important documents. Depending on the developer skills and understanding of cryptography, some types of ransomware can be decrypted without paying because of various flaws. However, most modern versions are not crackable and unfortunately, in those scenarios, decrypting the files is not usually possible.

More general information on this topic here: https://www.nomoreransom.org/en/ransomware-qa.html

For this assignment, you will have to analyze a toy implementation of a pseudo-malicious ransomware (it does not encrypt anything except for some circumstances you will discover). Moreover, for didactic reasons, this binary is fundamentally flawed from a cryptographic point of view such that even if encryption is triggered, decryption can be done with ease after proper analysis of the encryption algorithm.

Download the binaries from here[1]. The archive password is infected and has the following contents:

- asg1 - the binary you will analyze
- c19cf21d23c2a054462451047b202711 - the encrypted file you have to recover

2 Tasks

Perform the following tasks:

- The binary searches for files with a certain pattern and only encrypts those that match. Find out what the pattern is. (20p)
- Describe how the encrypted files are internally structured (what bytes are written in the encrypted files and how the encryption is done). (50p)
- Figure out how the file renaming process works and describe how decryption could theoretically be done. (20p)
- Create a program/script that decrypts any given encrypted file including the target file in the archive. (10p)

[1] https://pwnthybytes.ro/unibuc_re/asg1-files.zip

3 What to send

For the grading, you need to send:

- Detailed descriptions of what you did to solve each objective.
- Any logs/traces you consider important in your analysis.
- The IDB/I64 (or the IDC and screenshots if that's the case) resulting from your analysis in IDA Pro.
- The source code for your decryption program/script.
- The final decrypted file.

4 Where/when to send

There will be a Homework Assignment added to the Microsoft Teams channel. You will be able to send all your files and get feedback there.

The assignment can be solved until the 23rd of April 2023, 23:59 (hard deadline).