Computer Science Department, University of Crete

CS-457

Introduction to Information Security Systems

Spring Semester 2022

Reverse Engineering Lab

Due Date: 04/03/2022

Instructions

In order to access the assignment files, you should extract the three files from the zip then run ./unlock and enter your university ID to unlock the files (including “csd”, ex. csd4178). The only files needed for the assignment are the unlocked files **mal** and **dbb4fdbba0f4bb8b441c1d610260bbc8.VBR**.

You are instructed to use one of the following Reverse Engineering tools for your analysis:

- IDA Free (download)
- Ghidra (JDK 11) (download)
- Cutter (download)

You **do not** need to run the **mal** executable in order to answer the questions.

Description

You are a Cyber Incident Response Analyst working at an IT company. Your job is to analyze and collect information about recent cyber-attacks.

You are called in to a recent ransomware attack. An employee from the company downloaded and ran an untrusted executable which encrypted the company’s data and left a ransomware note.

You are given the ransomware executable and a copy of an encrypted file that the company would like to have decrypted as it contains useful login data. You are requested to:

- Write a report containing the findings of your analysis of the ransomware
- Optionally, write a script or a program that decrypts the encrypted files

Tasks

Write a detailed report in PDF format containing all your answers to the following questions. Provide **at least one** screenshot for **each** of them.

Overview

A. What kind of file is the ransomware? What architecture is it targeting and what command did you use to find this?

B. What is in the encrypted file? What note did the attackers leave behind?

Analysis

A. What kind of anti-analysis protection does the program use? What does it protect against?

B. What is the name of the function that contains the main ransomware activity?

C. What is the original name of the file that was encrypted by the ransomware?

D. What does the function you found in (B) do?

E. Discover the type of encryption that the ransomware applies on the original file and explain in detail the algorithm used.

F. Is the encryption algorithm reversible? Can we somehow get the original contents of the encrypted file back? If so, explain how in detail.

G. What does the ransomware append to the encrypted file after it is encrypted?

H. What is the new name of the encrypted file that the ransomware produces?

Decryption

A. In any programming language of your choice, implement a script or a program that takes the encrypted file as input and retrieves the original contents. Provide the full source code as well as the original file contents.

Submission

Submission will be done using the turnin system. You will be informed via the hy457 list when submissions are open.