Cybersecurity Piscine

Stockholm

Summary: Introduction to file manipulation by creating a harmless malware.

Version: 1

Contents

Chapter I

Prologue

Stockholm syndrome is a condition in which hostages develop a psychological bond with their captors during captivity. Stockholm Syndrome results from a rather specific set of circumstances, namely the power imbalances contained in hostage-taking, kidnapping, and abusive relationships. Therefore, it is difficult to find a large number of people who experience Stockholm Syndrome to conduct studies with any sort of power. This makes it hard to determine trends in the development and effects of the condition.

Emotional bonds may be formed between captors and captives, during intimate time together, but these are generally considered irrational in light of the danger or risk endured by the victims. Stockholm syndrome has never been included in the Diagnostic and Statistical Manual of Mental Disorders or DSM, the standard tool for diagnosis of psychiatric illnesses and disorders in the US, mainly due to the lack of a consistent body of academic research. The syndrome is rare: according to data from the FBI, about 5% of hostage victims show evidence of Stockholm syndrome.

This term was first used by the media in 1973 when four hostages were taken during a bank robbery in Stockholm, Sweden. The hostages defended their captors after being released and would not agree to testify in court against them.[3] It was noted that in this case, however, the police were perceived to have acted with little care for he hostages' safety,[7] providing an alternative reason for their unwillingness to testify. Stockholm syndrome is paradoxical because the sympathetic sentiments that captives feel towards their captors are the opposite of the fear and disdain which an onlooker might feel towards the captors.

Source: https://en.wikipedia.org/wiki/Stockholm_syndrome

Chapter II

Introduction

In this project you will develop a small program with the aim of understanding how malware works.

We will focus on ransomware.

A specific feature of this type of program is its ability to spread through networks of hundreds of computers. In our case, your program will only affect a small portion of your local files. It's all about understanding how a fairly simple program works in order to better protect yourself from it.

> ⚠ `This project is for educational purposes only. You should never use this type of program for malicious purposes.`

Chapter III

Mandatory Part

This project is for educational purposes only. You should never use this type of program for malicious purposes.

You must work in a virtual machine or in docker with the distribution of your choice. We will stay in a linux environment.

You must create a program called `stockholm` with these specifications:

- It must be developed for the Linux platform.
  - The program must have the option "–help" or "-h" to display the help.
  - The program must have the option "–version" or "-v" to show the version of the program.
  - The program must have the option "–reverse" or "-r" followed by the key entered as an argument to reverse the infection.
  - The program must show each encrypted file during the process unless the option is indicated "–silent" or "-s", in which case the program will not produce any output.
- The program have to handle errors and will not stop unexpectedly in any case.

Your program must perform several actions described below:

- It must only work in a folder called `infection` in the user's HOME directory.
- The program will only act on files whose extensions have been affected by Wannacry.

`You'll have to do a little research on this!`

- The program have to encrypt the contents of the files in this folder using a key.
- Files must be encrypted with a known algorithm of your choice, which is considered secure.
- The program must rename all the files in the mentioned folder adding the ".ft" extension.
- If they already have this extension, they will not be renamed.
- The key with which the files are encrypted will be at least 16 characters long.
- The program must be able to do the reverse operation using the encryption key in order to restore the files to their original state.

To make this program you can use any language you want. However:

- You must add a file of maximum 50 lines called README.md to the root of your repository. This file should contain instructions for use and, if necessary, for compilation.
- You must add to the root of your repository a Makefile to configure the files so that the program can be run.
- In any case, you must include all the source code of the program.

`You can use encryption libraries such as openssl or libsodium, but you need to justify your choice of encryption during the evaluation.`

`This project is for educational purposes only. You should never use this type of program for malicious purposes.`

Chapter IV

Submission and peer-evaluation

Turn in your assignment in your `Git` repository as usual. Only the work inside your repository will be evaluated during the defense. Don't hesitate to double check the names of your folders and files to ensure they are correct.