German University in Cairo
Department of Computer Science
Faculty of MET - CSEN 1001
Dr. Amr El Mougy
Meriam Khalifa
Ahmed Mazhr

Computer and Network Security, Spring 2023
Project : Ransomware

Due: May 18th by 23:59

1. Introduction

In this project you are required to develop a ransomware using python. This can be done using encryption and client-server architecture in order to be able to exchange data between the attacker and the victim.

2. Overview Your main goal is to write a malware that does the following:

- Generate a random 128 bit key (16 characters) using ascii characters.
- Find all *.txt* files on the victim's computer and Encrypt the bytes of these files.
- Send that key back to the server.
- Infect by sending your compiled malware to a list of emails.

3. Requirements

- **Payload**
  a) Encrypt ALL .txt files on the system.
  b) Use AES (choose any mode) for the encryption process with the random key mentioned at the beginning.
  c) Generate a Public/Private key-pair using RSA
  d) Save the key used in (b) to desktop in a *.key* (normal text file but change the extension to .key not to mistakenly re-encrypt it) format named "*Key.key*".
  e) Encrypt the key used in (b) using the public key then save the encrypted key to the desktop in a *.key* file format named "*encryptedKey.key*".
  f) Save the generated Public/Private key pair (one key per line ,Public then Private) in another *.key* file named "*keyPair.key*".
  g) Send the encrypted key from (e) to the server.
  h) A decryption function must be present and will decrypt all files when the original key is entered.
- **Infection**
  a) You should add an infection mechanism that sends the .exe file to the emails below.
  b) Your code should access the following csv , extract the emails from it then send the .exe file to them. https://docs.google.com/spreadsheets/d/1Wcb2hzqL56QorxwBFW96QW
  out : *csv* (do not hardcode the emails)

- **Interface**
  a) A prompt should popup (CLI or GUI) indicating that the encryption is in progress when the .exe is executed.
  b) After encrypting all txt files, the prompt will wait for a key input in order to decrypt the files back. Ënter Key to decrypt"

4. Setup

- You need to set up a virtual environment that will act as the client i.e the victim computer. In order to be able to run this virtual machine you have to install windows 10 ISO disc image on it that can be downloaded using "Windows media creation tool"which you can download from Microsoft website using the following link: https://www.microsoft.com/en-us/software-download/windows10
- After setting your environment up, you are required to download the "*Starter-Code.zip*"folder from the CMS, extract it and write your implementation in "*Client.py*"file.
- After writing your malware , use auto-py-to-exe library to convert *Client.py* file into a .exe file then copy this file into the virtual machine in order to be able to run the ransomware.

5. Submission

a) Your finished ransomware must be submitted as a working .exe file
b) A Report with team name and members w/ ID and tutorial number.
c) The report must include a block diagram for the encryption/decryption along with their functions.
d) Zip the report , your .exe file and source code all in one file to submit it.

6. IMPORTANT NOTES

a) **NEVER** run the ransomware on your computer; you should setup the windows virtual machine and work there, otherwise you will loose all of your files.... we are not responsible.
b) If any of windows security components blocks your malware executable: disable them. (Google is your friend)
c) You should implement your work in python.
d) Google is your friend.
e) You must stick to the naming conventions of the files since they will be automatically graded
f) Goo..

7. Important Dates

Team Submission Make sure you submit your team details by April 30th at 23:59 using the following link `https://forms.gle/XysqCch7ZWz4iWc18`. Only one team member should submit this for the whole team. After this deadline, we will be posting on the CMS a team ID for each submitted team. You will be using this team ID for submission.

Source code and Project Report On-line submission by May 18th at 23:59. The submission details will be announced after the team submission deadline.