

## 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.

## 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 (128-bit key).
- 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.

### • Interface

- a) A prompt should pop-up (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. Enter Key to decrypt"

## 4. Setup

- You need to set up a virtual environment that will act as the client i.e the vic-tim 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.