Ransomware Report

# How to run:

1. Make sure you have python3 and pycryptodome installed on your Linux/Unix machine. Use the following commands in terminal, to install python3 and pycryptodome if you have not:
   1. sudo apt-get update
   2. sudo apt-get install python3.6
   3. sudo apt-get install build-essential python3-dev python3-pip
   4. pip3 install pycryptodome
2. Put zipped folder into an easy to access directory and unzip it.
3. Use console commands to navigate to the directory inside the unzipped folder.
4. Make sure the folder includes ransomware\_part\_one.py, victim\_address.txt, victim\_bank\_login.txt, victim\_credit\_card.txt, key\_recovery.py and file\_recovery.py.
5. Open the terminal and type in or copy, one at a time:
   1. python3 ransomware\_part\_one.py
   2. python3 key\_recovery.py
   3. python3 file\_recovery.py

# Packages:

* default:
  + glob (get list of only victim files in the current directory)
  + os (get a list of all files in the current directory)
  + sys (get the python file name (argument) that was executed in terminal)
* pycryptodome
  + Crypto.Cipher
    - AES (used for symmetric encryption of data in text files)
    - PKCS1\_OAEP (a cipher used for encryption and decryption)
  + Crypto.PublicKey
    - RSA (used for public key encryption of key)
  + Crypto.Util.Padding
    - pad (used to pad data to make sure it is correct bit size for encryption)
  + Crypto.Random
    - get\_random\_bytes (get random bytes to create 256 bits key)
* base64
  + b64encode (encode a byte like object)
  + b64decode (decode a byte object to a string)

# Execution Screenshots:

(You will need to zoom in to see the image better)

1. Graphical user interface

   Description automatically generatedThe directory will initially have the ransomware program and the victims text files.
   1. The ransomware program is executed.
   2. It encrypts the victims text files using symmetric encryption, deletes the victim’s text files and creates new .enc files that the encrypted text from each victim’s text file is stored.
   3. It creates a key.bin file where the key used for symmetric encryption of text files, is encrypted using public key encryption and stored.
   4. It creates a ransomprvkey.pem file where the private key is stored.
   5. It creates a file ransomware\_propagation.py where it copies itself to.
   6. Graphical user interface, application

      Description automatically generatedIt comments its own code out.

Graphical user interface, text, application, email

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generated

Graphical user interface, application

Description automatically generated

* 1. The victim will need to send payment of $5000 and the key.bin file to the specified email address.
  2. Once I receive the payment, I will send a key recovery program and then file recovery program.
  3. The key recovery program uses the private key stored in ransomprvkey.pem, to decrypt the key in key.bin.
  4. It encodes the decrypted key to base 64.
  5. It creates a new text file key.txt, where the decrypted base 64 encoded key is stored.

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

* 1. The file recovery program is then run.
  2. It decodes the decrypted key and applies symmetric key decryption to decrypt the victim’s text files.
  3. It deletes the .enc files.
  4. Graphical user interface, application

     Description automatically generatedGraphical user interface, application

     Description automatically generatedIt creates new .txt files to store the decrypted text that is the text from the victim’s original text files.