Asignatura:

LABORATORIO ALGORITMOS MALICIOSOS

Participantes:

Angel Manuel Dipre Mateo 1116417

Proyecto Final

Facilitador:

Harold Lawrence Marzan Mercado

Fecha:

25/01/2025

Documentación de MondongoNetRam

Descripción General

Este programa utiliza técnicas de criptografía para cifrar y descifrar archivos en carpetas específicas del sistema. Además, genera una clave única para el cifrado de los archivos, la cual es enviada al correo electrónico configurado en el programa. El programa incluye una interfaz gráfica (GUI) desarrollada con Tkinter que permite al usuario interactuar con las funciones principales de cifrado y descifrado.

Advertencia

Este programa es estrictamente para fines educativos. El uso indebido de este programa puede tener consecuencias legales. No utilices este software con fines maliciosos.

Paquetes Utilizados

1. **cryptography.fernet**: Implementa cifrado seguro usando el algoritmo AES con autenticación HMAC.
2. **os**: Permite interactuar con el sistema operativo para manejar archivos y directorios.
3. **tkinter**: Proporciona herramientas para la creación de interfaces gráficas.
4. **smtplib**: Permite el envío de correos electrónicos a través del protocolo SMTP.
5. **email.mime**: Facilita la construcción y formateo de mensajes de correo electrónico.

Descripción de las Funciones

1. send_key_via_email(key)

- Envía la llave de cifrado generada al correo del atacante configurado.
- Usa el protocolo SMTP para conectarse a un servidor de correo y enviar la llave.
- Parámetro:
    - key: Clave de cifrado generada por el programa.

2. create_ransom_note()

- Genera un mensaje con las instrucciones de rescate que incluye:
    - El monto a transferir.
    - El número de cuenta del atacante.
- Retorna una cadena con las instrucciones.

3. encrypt_file(file_path, key)

- Cifra un archivo dado utilizando la clave proporcionada.
- Sobrescribe el archivo original con la versión cifrada.
- Parámetros:
    - file_path: Ruta del archivo a cifrar.
    - key: Clave de cifrado generada.

4. decrypt_file(file_path, key)

- Desencripta un archivo dado utilizando la clave proporcionada.
- Sobrescribe el archivo cifrado con su versión descifrada.

- Parámetros:
    - file_path: Ruta del archivo a descifrar.
    - key: Clave de descifrado.

5. encrypt_folder(folder_path, key)

- Recorre todos los archivos dentro de una carpeta y aplica la función de cifrado.
- Parámetros:
    - folder_path: Ruta de la carpeta cuyos archivos serán cifrados.
    - key: Clave de cifrado.

6. decrypt_folder(folder_path, key)

- Recorre todos los archivos dentro de una carpeta y aplica la función de descifrado.
- Parámetros:
    - folder_path: Ruta de la carpeta cuyos archivos serán descifrados.
    - key: Clave de descifrado.

7. ransomware_window(key, folders_to_process)

- Crea una ventana gráfica persistente que solicita al usuario la llave de descifrado.
- No permite cerrar la ventana hasta que se introduzca la clave correcta.
- Parámetros:
    - key: Clave de descifrado generada por el programa.
    - folders_to_process: Lista de carpetas cuyos archivos serán descifrados.

8. ransomware_encrypt()

- Es la función principal del programa. Realiza las siguientes tareas:

1. Genera una clave única de cifrado.
2. Envía la clave al correo configurado.
3. Cifra los archivos en las carpetas especificadas.
4. Muestra la ventana gráfica con las instrucciones de rescate y la opción para ingresar la clave.

Flujo de Trabajo del Programa

1. **Inicialización**:
    - Configura las carpetas objetivo donde se cifrarán los archivos.
    - Genera una clave única de cifrado usando la biblioteca cryptography.
2. **Envío de la Clave**:
    - Envía la clave generada al correo electrónico del atacante mediante SMTP.
3. **Cifrado**:
    - Recorre las carpetas especificadas y cifra todos los archivos en ellas.
4. **Interfaz Gráfica**:
    - Muestra una ventana que no se puede cerrar, con las instrucciones de rescate.
    - Permite al usuario ingresar la clave para descifrar los archivos.
5. **Descifrado**:
    - Si la clave ingresada es correcta, los archivos son descifrados y restaurados a su estado original.

Configuraciones Específicas

Correo Electrónico

- Configura las credenciales del correo en la función send_key_via_email:
    - **Correo remitente:** your_email@example.com.
    - **Contraseña:** your_password.
    - **Correo del atacante:** attacker@example.com.

Carpetas a Cifrar

- Define las carpetas objetivo en la función ransomware_encrypt:
- folders_to_encrypt = [
- "C:\\Ataque",
- "C:\\Documentos",
- "C:\\Trabajo"
-]

Dependencias

Asegúrate de instalar las bibliotecas necesarias con:

```
pip install cryptography tkinter
```

Advertencia Final

Este programa está diseñado exclusivamente para fines educativos. No está permitido utilizar este software para actividades malintencionadas o ilegales. El uso indebido del programa puede tener graves consecuencias legales y éticas.