

Introducción al Proyecto: Simulated-Ransomware-Hybrid-Encryptor_Fernet-and-Azar_encryptor

Este proyecto tiene fines ****educativos**** y busca demostrar cómo funciona un sistema de ****cifrado híbrido de archivos****, simulando el comportamiento de un ransomware ético. Está diseñado para enseñar conceptos clave de criptografía aplicada, manipulación de archivos, y envío seguro de metadatos.

¿Cómo funciona?

El proceso de cifrado se realiza en dos capas:

1. ****Cifrado simétrico con Fernet (AES):**** protege el contenido original del archivo.
2. ****Cifrado personalizado Azar_Encryptor:**** aplica una sustitución aleatoria a nivel de bytes para añadir una capa adicional de ofuscación.


Los metadatos necesarios para el descifrado (alfabeto, desplazamientos y clave) se almacenan comprimidos y se envían automáticamente por correo electrónico. Luego, el descifrado requiere esos metadatos y la clave Fernet para restaurar los archivos originales.

Objetivos del proyecto

- Enseñar técnicas reales de cifrado de archivos.
- Simular de forma segura el flujo de un ransomware.
- Incentivar el análisis ético y técnico de la criptografía híbrida.
- Servir como base para proyectos académicos o pruebas controladas de seguridad.

 ****Este proyecto no debe ser usado para fines maliciosos. Su propósito es exclusivamente académico y experimental.****

Enlaces

-  Repositorio en GitHub: https://github.com/dapach7/Simulated-Ransomware-Hybrid-Encryptor_Fernet-and-Azar_encryptor
-  Video explicativo: <https://youtu.be/huXS9gZfoX8>