Ejercicio:
Visite la página:
https://www.welivesecurity.com/la-es/2020/07/29/analisis-codigo-fuente-ransomware-escrito-python/
y responda a estas preguntas:

1. ¿Qué algoritmo se usa el ransomware para cifrar los archivos?
   El ransomware utiliza el algoritmo de cifrado AES 256 en modo CBC (Cipher Block Chaining) para cifrar los archivos.
2. ¿Es un algoritmo simétrico o asimétrico?
   El algoritmo utilizado, AES 256, es un algoritmo de cifrado simétrico. Esto significa que utiliza la misma clave para cifrar y descifrar los archivos.
3. ¿Qué motivo puede haber llevado al programador del malware a usar dicho algoritmo?
   La elección del algoritmo simétrico AES 256 puede deberse a su robustez y eficiencia en términos de rendimiento. AES es ampliamente utilizado y considerado seguro, lo que hace que sea más difícil para las víctimas descifrar los archivos sin la clave adecuada.
4. ¿Se pueden recuperar los datos sin necesidad de pagar el rescate? Razone su respuesta basándose en lo que sabe sobre algoritmos simétricos y asimétricos.
   En teoría, es posible recuperar los datos sin pagar el rescate si se cuenta con la clave de cifrado. En este caso, la clave se genera a partir del identificador de la computadora de la víctima, y esta información está presente en la propia computadora. Además, como se menciona en la conclusión, programar un script que extraiga los datos necesarios y descifre los archivos podría ser una opción para recuperar los archivos sin depender del cibercriminal. Sin embargo, este proceso puede ser técnico y no es garantía de éxito en todos los casos.

Por curiosidad, en la siguiente página web hay una lista de ransomwares que han sido descifrados:
https://www.nomoreransom.org/es/index.html

Lea el siguiente artículo:
https://www.muyseguridad.net/2020/08/05/garmin-pago-descifrar-wastedlocker/

5. ¿Por qué este ransomware no puede ser descifrado si no se paga rescate? Piense en la forma en la que se pueden mezclar cifrado simétrico y asimétrico para conseguir este objetivo.

6. Piense ahora en formas en la que el ransomware se puede propagar y enumérelas. En el siguiente enlace tiene un ejemplo:

https://forococheselectricos.com/2020/08/un-hacker-ruso-es-detenido-por-ofrecer-un-millon-de-dolares-a-un-empleado-de-tesla-para-instalar-malware-en-la-gigafabrica-de-nevada.html