Práctica 4 – Desarrollo de Herramientas de Ciberseguridad – Ransomware

Introducción: se ha desarrollado un software tipo ransomware capaz de cifrar los archivos con uso de multihilo de un directorio y de sus respectivos subdirectorios usando un algoritmo XOR y luego sobrescribiendo en el mismo fichero en formato hexadecimal.

No se ha realizado la parte del C2 debido a una falta de tiempo provocada por más prácticas de otras asignaturas, pero cabe decir que esta ha sido de las prácticas que más me ha gustado hacer y seguiré mejorándola en mi tiempo libre.

Lógica y métodos utilizados:

- Función **encrypt_directory_files:** navega de manera recursiva entre los subdirectorios identificando los ficheros para poder cifrarlos.
  Crea una variable tipo DIR para poder manejar el directorio recibido por parámetro el cual se analizará identificando todas las entradas gracias a la librería #include <sys/stat.h> y detectando los directorios cuando la macro S_ISDIR devuelve 1 para volver a llamarse a la función misma pero enviando por parámetro el directorio detectado creando así la recursividad del software o en el caso de que la entrada al procesarse con la macro S_ISREG sea un fichero regular se llamará a la función de cifrado para encriptarlo.

- Función **encrypt_file:** abre el fichero que se quiere cifrar en modo lectura como infile par almacenar en un buffer todos sus bytes, se divide el contenido del buffer en 8 bloques, uno por cada hilo. Se ha usado la función hardware_concurrency para ver cuantos hilos soporta el dispositivo en el que se va a ejecutar el software, como mi portátil soporta 8 hilos pues por eso son 8 los bloques. Se crean los hilos y se les envía por parámetro tanto la función de cifrado de cada bloque de manera independiente como la referencia al buffer para que se cambien los datos legibles por los cifrados.
  Se espera a que finalicen todos los hilos para la correcta sincronización de estos y se abre de nuevo el fichero, pero en este caso en modo escritura para poder sobrescribir los bytes del buffer ya cifrados usando la función write_hex.

Por último se renombra el fichero cifrado añadiéndole “.enc” al final para mostrar que el fichero ha sido encriptado con la función rename.

- Función **encrypt_block:** es la función que ejecuta cada hilo en paralelo y consiste básicamente en aplicar el algoritmo de cifrado XOR a cada byte del buffer. Una vez cifrado, se actualiza el byte del buffer para más tarde, en la función de encrypt_file poder sobrescribirlo en el fichero.

- Función **write_hex:** escribe en el fichero de salida enviado por parámetros los bytes del buffer también obtenido por parámetros en formato hexadecimal.

- Función **main:** obtiene por parámetro del ejecutable el directorio que se quiere cifrar, se define la clave de cifrado y se llama a la función recursiva encrypt_directory_files.

Diagrama de flujo