Writeup P1 Tarea 3

Writeup P1 Tarea 3

Nombre: Benjamín Aguilar Osorio
Equipo: L05 1NCR31BL35

Persona a cargo de la pregunta **Joaquín Oportus**

Descripción general del problema

Se trata de un problema de forense, donde se entrega una imagen de un sistema operativo (SO) presuntamente afectado por un ransomware.

Metodología de resolución

A continuación se darán los **pasos** que se llevaron a cabo para resolver el problema:

1. En una revisión inicial del problema, se puede determinar que se tiene un archivo que corresponde a una imagen de un sistema operativo (SO) supuestamente corrupto por un ransomware.
2. Siguiendo el hint del compañero a cargo del problema, se optó por el uso de Autopsy para el análisis de la imagen del disco.
3. Al utilizar la herramienta Autopsy, se pudo acceder a los archivos de la imagen, donde se analizaron los discos C y D. En particular, en el disco D, gracias a la herramienta de búsqueda por nombre de archivo de Autopsy, se pudieron encontrar varios archivos con el nombre "flag", pero específicamente uno que estaba presente en el escritorio del usuario Sysuser.
4. Al acceder al escritorio del usuario mencionado, se encontraron más archivos. Por un lado, se encontró un archivo que probablemente tuviera la flag, pero estaba corrupto. Y por otro lado, se encontró un archivo "read me" cifrado en hexadecimal. Mediante el uso del visor hexadecimal de Autopsy, se pudo obtener un texto que explicaba cómo "recuperar" los datos mediante un pago utilizando un servidor de Tor.
5. Sin tener todavía idea del ransomware utilizado, se revisaron nuevamente los demás archivos con el nombre "flag", examinando los directorios correspondientes. En particular, se encontró el directorio D:/Users/Sysuser/AppData/Roaming/Microsoft/Windows/Recent/flag.txt.lnk.
6. Al acceder a la dirección mencionada, se encontró un archivo con el nombre "DFIR_Resources_REvil_Kaseya-main". Al buscar este archivo en Google, se obtuvo la dirección del siguiente repositorio en GitHub: https://github.com/cado-security/DFIR_Resources_REvil_Kaseya. En este repositorio se mencionaba este archivo como un ransomware y se explicaba su funcionamiento.

7. Teniendo ya el tipo de ransomware, se consultó con el integrante encargado del problema por algún programa que pudiera recomendar. Él recomendó Bitdefender.
8. Después de descargar Bitdefender y leer un poco sobre su funcionamiento, se descargaron los archivos "flag.txt" y "readme" del escritorio del usuario Sysuser, y se los proporcionó al programa mencionado anteriormente.
9. El programa logró recuperar el archivo "flag.txt", obteniendo de esta manera un texto cifrado en base64 (**Q0M1MzI1e1I0bnMwbXc0cjNfZDNjcnlwNzByfQ==**), que gracias a la ayuda de CyberChef se pudo convertir en la flag: **CC5325{R4ns0mw4r3_d3cryp70r}**.