Análisis de Malware

La primera parte consiste en el análisis de dos ejecutables de Windows proporcionados. Se proporciona una carpeta con el nombre MALWR2.zip en CANVAS, la cual posee la contraseña *infected*

Se sugiere utilizar una VM con Linux para trabajar. Se debe descargar el archivo y descomprimirlo en la ubicación deseada. Luego se debe descomprimirlo y NO se debe manipular manualmente ningún archivo, de hacerlo se corre el riesgo de ejecutarlo e infectarse.

NOTA: se proporcionan ejemplos reales de malware, para efectos de aplicar los conocimientos académicos de análisis estático y dinámico de malware, y es responsabilidad del alumno(a) cualquier uso adicional que no sea el indicado en este laboratorio. Luego de finalizar el laboratorio se deben eliminar todos los ejemplares.

Parte 1 – análisis estático

1. Utilice la herramienta pefile para examinar el PE header y obtenga las DLL y las APIs que cada uno de los ejecutables utilizan. ¿Qué diferencias observa entre los ejemplos? ¿Existe algún indicio sospechoso en la cantidad de DLLs y las APIs llamadas?
2. Obtenga la información de las secciones del PE Header. ¿Qué significa que algunas secciones tengan como parte de su nombre “upx”? Realice el procedimiento de desempaquetado para obtener las llamadas completas de las APIs.
3. Según el paper “Towards Understanding Malware Behaviour by the Extraction of API Calls”, ¿en que categoría sospechosas pueden clasificarse estos ejemplos en base a algunas de las llamadas a las APIs que realizan? Muestre una tabla con las APIs sospechosas y la categoría de malware que el paper propone.
4. Para el archivo “sample_vg655_25th.exe” obtenga el HASH en base al algoritmo SHA256.
5. Para el archivo “sample_vg655_25th.exe”, ¿cuál es el propósito de la DLL ADVAPI32.dll?
6. Para el archivo “sample_vg655_25th.exe”, ¿cuál es el propósito de la API CryptReleaseContext?
7. Con la información recopilada hasta el momento, indique para el archivo ““sample_vg655_25th.exe” si es sospechoso o no, y cual podría ser su propósito.

Parte 2 – análisis dinámico

8. Utilice la plataforma de análisis dinámico https://www.hybrid-analysis.com y cargue el archivo “sample_vg655_25th.exe”. ¿Se corresponde el HASH de la plataforma con el generado? ¿Cuál es el nombre del malware encontrado? ¿Cuál es el propósito de este malware?
9. Muestre las capturas de pantalla sobre los mensajes que este malware presenta a usuario. ¿Se corresponden las sospechas con el análisis realizado en el punto 7?