Universidad del Valle de Guatemala
Facultad de Ingeniería
Departamento de Ciencias de la Computación

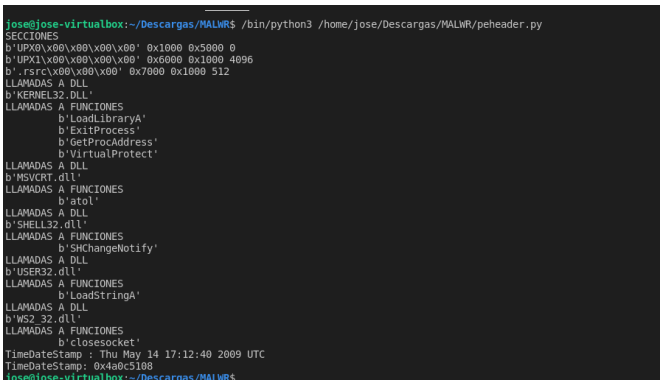
HDT Análisis de Malware

Jose Pablo Ponce 19092

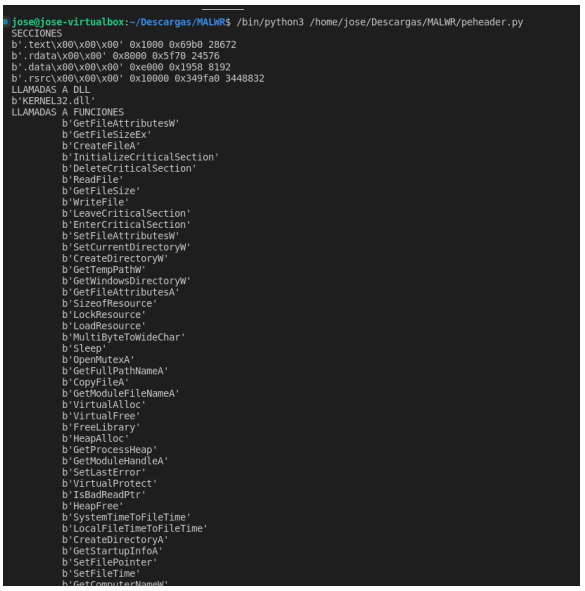
Hoja de Trabajo

Parte 1 – análisis estático

sample_qwrty_dk2



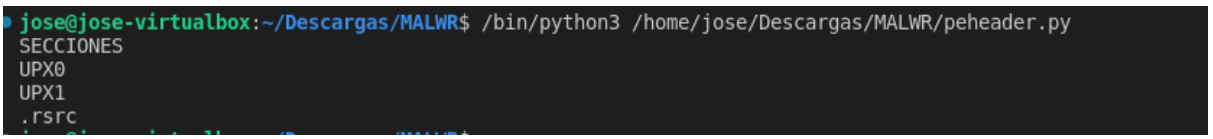
sample_vg655_25.th



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?

Se puede observar que la cantidad de llamadas a DLLs y APIs es diferente, por otro lado un indicio puede ser que existan muy pocas llamadas a Apis en el archivo sample_qwrty_dk2.

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.



La presencia de upx significa que el archivo fue comprimido y luego empacado dentro del ejecutable con UPX.

3. Según el paper “Towards Understanding Malware Behaviour by the Extraction of API Calls”, ¿en qué 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.

comportamiento	categoria de malware	llamadas a API
1	buscar archivos a infectar	FindClose, FindFirstFile, FindFirstFileEx
2	copiar/eliminar archivos	CloseHandle, CopyFile, CopyFileEx, CopyFileTransacted, CreateFile, CreateFileTransacted, CreateHardLink
3	obtener informacion de archivos	GetBinaryType, GetCompressed, FileSize, GetCompressedFile, SizeTransacted, GetFileAttributes, GetFileAttributesEx, GetFileAttributes, Transacted
4	mover archivos	Behaviour 4 Move Files MoveFile, MoveFileEx, MoveFileTransacted, MoveFileWithProgress
5	leer/escribir archivos	OpenFile, OpenFileById, ReOpenFile, ReplaceFile, WriteFile, CreateFile, CloseHandle
6	cambiar atributos de archivos	SetFileApisToANSI, SetFileApisToOEM, SetFileAttributes, SetFileAttributesTransacted, SetFileBandwidthReservation,

		SetFileInformationByHandle, SetFileShortName, SetFileValidData

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?

Es una biblioteca que proporciona funciones relacionadas a la seguridad, la autenticación y la administración de cuentas. Por ende cualquier modificación con la dll puede tener un impacto significativo en el rendimiento del sistema operativo

6. Para el archivo “sample_vg655_25th.exe”, ¿cuál es el propósito de la API CryptReleaseContext?

Crear un contexto de criptografía y devolver un identificador de contexto para poder realizar operaciones criptográficas de encriptación y desencriptación y verificación de firmas.

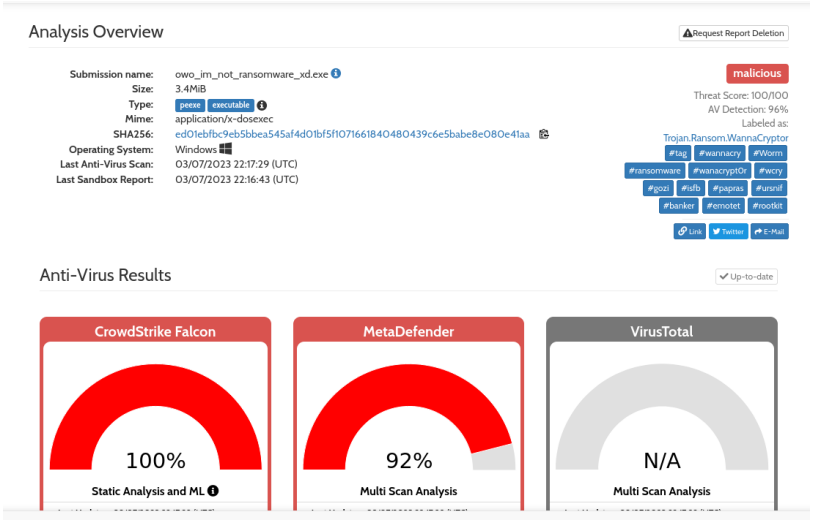
7. Con la información recopilada hasta el momento, indique para el archivo ““sample_vg655_25th.exe” si es sospechoso o no, y cual podría ser su propósito.

Con lo recopilado hasta el momento, se puede tomar el archivo como sospechoso y que tiene como propósito afectar el rendimiento del sistema operativo y bloquear funciones del sistema operativo.

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?

Se puede observar que el HASH de la plataforma es el mismo que el generado y el propósito del malware es cifrar archivos de computadora y descifrarlos hasta que se realice un pago.



9. Muestre las capturas de pantalla sobre los mensajes que este malware presenta al usuario. ¿Se corresponden las sospechas con el análisis realizado en el punto 7?

Se puede observar que mi sistema operativo ya no está funcionando igual y que hay secuestro de información, ya que se cifra toda la información que se tenía y hay que pagar para obtenerla de vuelta.