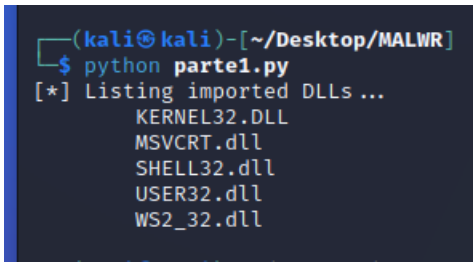
Hoja de Trabajo 2

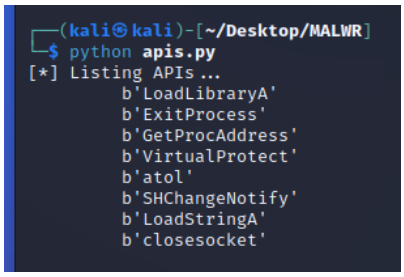
Andrea Amaya 19357

Parte 1.

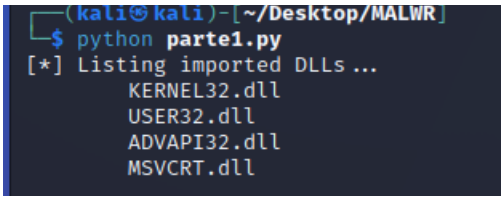
a. DLL y APIs

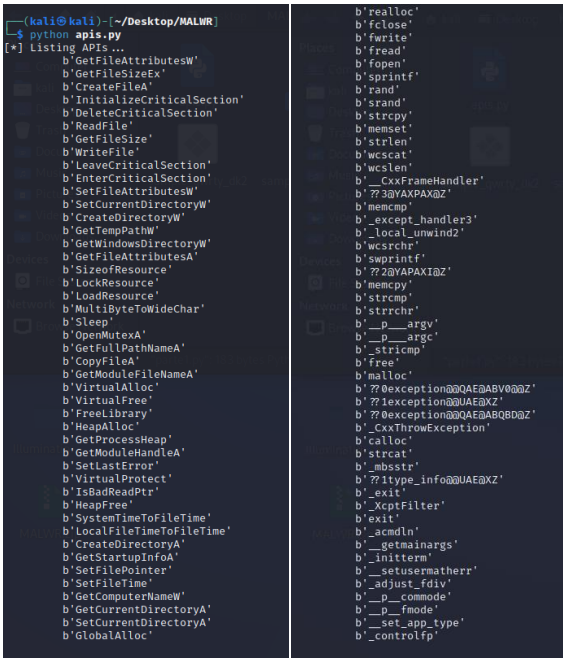
sample_qwrty_dk2





sample_vg655_25th.exe





¿Qué diferencias observa entre los ejemplos? ¿Existe algún indicio sospechoso en la cantidad de DLLs y las APIs llamadas? Al comparar los DLL entre ambos archivos, el único sospechoso es el WS2_32.dll el cual es un archivo ejecutable en el disco duro del ordenador. Ahora al comprar las llamadas API, el .exe contiene muchas más que el otro archivo. Y, al revisar el listado, en el .exe se encuentran nombres sospechosos como "??1type_info@@UAE@XZ" u otros que no son legibles para un humano. Al revisar los nombres de las llamadas, el primer archivo también cuenta con algunos nombres dudables como "LoadStringA" el cual probablemente intente modificar alguno de los archivos de inicio del Windows al tener el dll WS2_32.

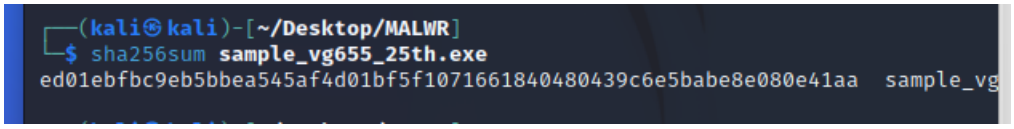
b. ¿Qué significa que algunas secciones tengan como parte de su nombre "upx"?

Upx es un compresor de archivos, lo cual hace que se salten los pasos de seguridad (antivirus) al estar comprimidos y no el archivo completo.

c. 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.

Nombre	Categoría
ReadFile, WriteFile, CreateDirectory	Read/Write Files
DeleteCriticalSection	Copy/Delete Files
GetFileAttributesW, GetFileSize	Search files to infect

d. Para el archivo "sample_vg655_25th.exe" obtenga el HASH en base al algoritmo SHA256.



e. Para el archivo "sample_vg655_25th.exe", ¿cuál es el propósito de la DLL ADVAPI32.dll?

ADVAPI32 hace referencia a los archivos esenciales del sistema operativo. Además, incluye APIs de llamadas de seguridad y registros. Cuando Advapi32.dll se corrompe o falta, empieza a provocar que el sistema informático se descontrole.

f. Para el archivo "sample_vg655_25th.exe", ¿cuál es el propósito de la API CryptReleaseContext?

Es la función encargada de liberar identificadores de proveedores de servicios criptográficos (CSP) y un contenedor de claves. Luego de esta función, el CSP y los objetos hash existentes ya no son válidos.

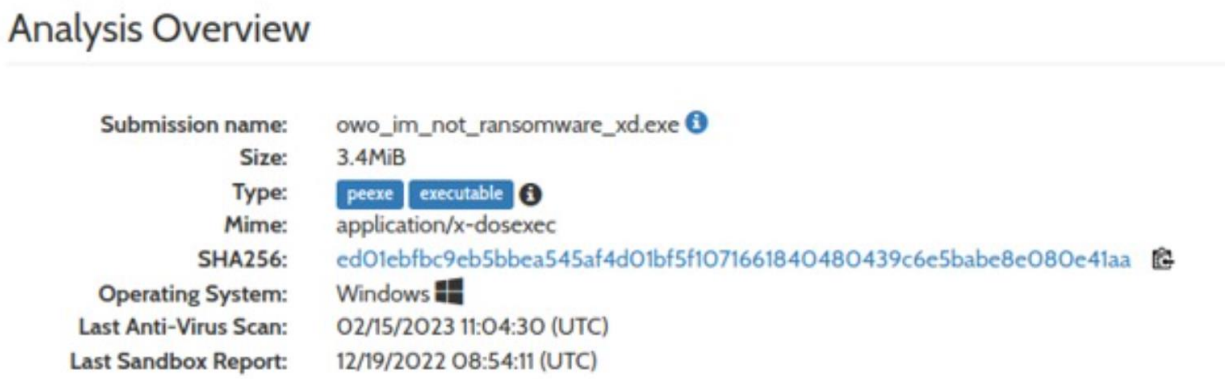
g. **Con la información recopilada hasta el momento, indique para el archivo ““sample_vg655_25th.exe” si es sospechoso o no, y cual podría ser su propósito.**

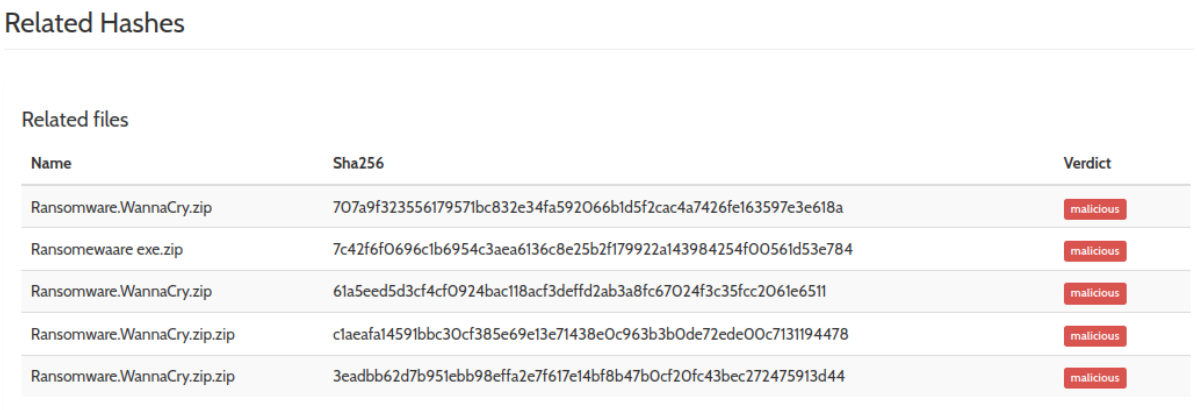
Sí es sospechoso, el posible propósito es que encripte la información del usuario de forma aleatoria hasta terminar todos los archivos y que ya no se pueda acceder a la máquina. Esto se debe a que los hash son invalidados al volver a llamar la función.

Parte 2.

a. **¿Se corresponde el HASH de la plataforma con el generado? ¿Cuál es el nombre del malware encontrado? ¿Cuál es el propósito de este malware?**

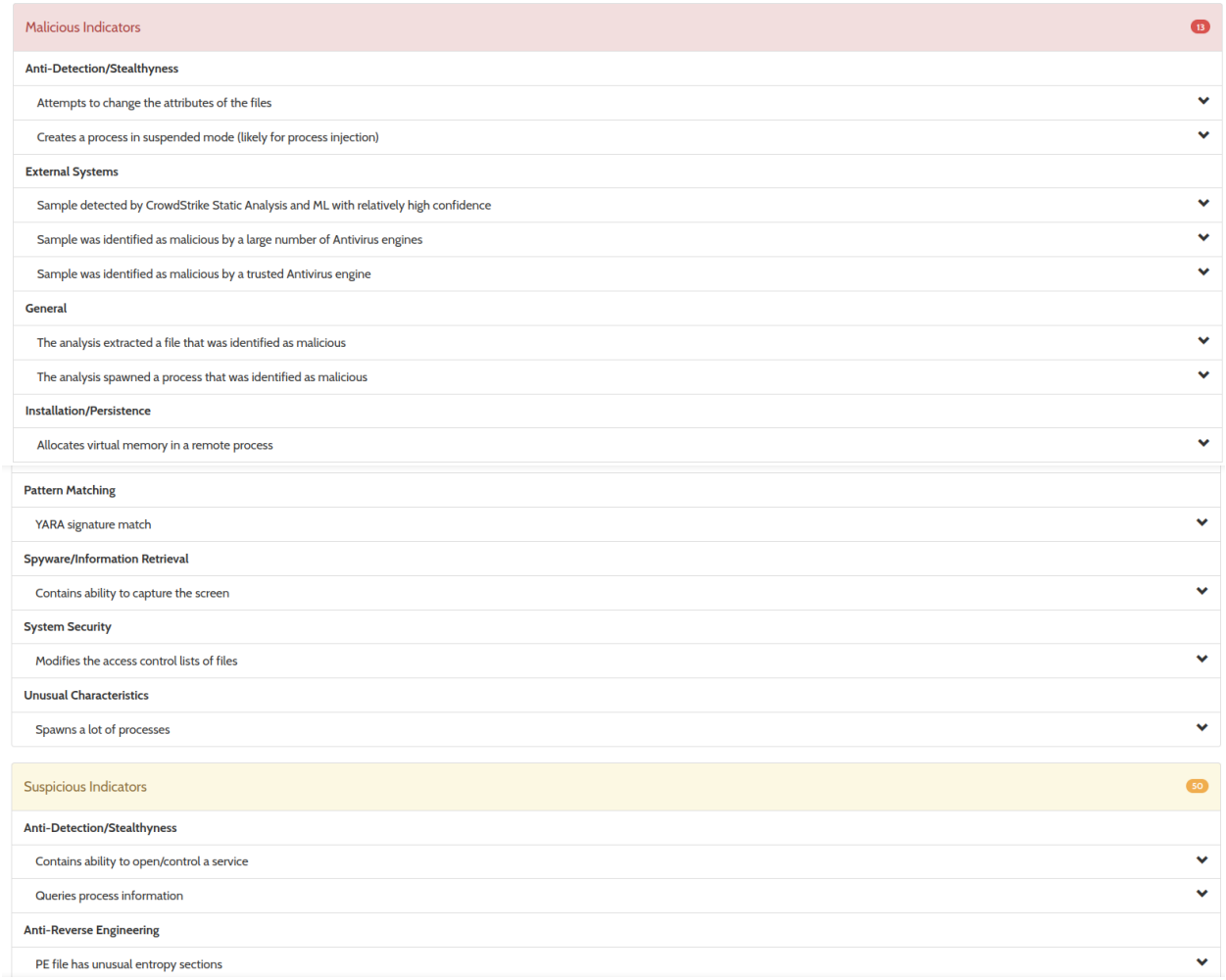
Sí corresponde el hash de la plataforma con el generado. El nombre del malware es owo_im_not_ransomware_xd.exe. El propósito del malware es obtener las llaves del sistema y eliminar grandes volúmenes de datos.





b. 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?

Según los mensajes obtenidos, el malware intenta cambiar archivos, inyección de procesos, cambia archivos de seguridad y genera una gran cantidad de procesos. Corresponde en ciertas partes, porque sí menciona que logra deshabilitar la reparación del dispositivo por medio del startup y que puede acceder a toda la información incluso por navegador web.



- An application crash occurred
- Calls an API typically used to copy file from one location to another
- Calls an API typically used to create a directory
- Calls an API typically used to create a process
- Contains ability to delay the execution of current thread
- Contains ability to dynamically load libraries
- Contains registry location strings
- Creates mutants
- Drops or executes a batch file
- Found API related strings
- Launches a VBS file
- Logged script engine calls
- Overview of unique CLSIDs touched in registry
- PE file contains executable sections
- PE file contains writable sections

Risk Assessment

Remote Access	Reads terminal service related keys (often RDP related)
Spyware	Accesses potentially sensitive information from local browsers Contains ability to open the clipboard Deletes volume snapshots (often used by ransomware) Hooks API calls
Persistence	Disables startup repair Grants permissions using icacls (DACL modification) Installs hooks/patches the running process Spawns a lot of processes Tries to suppress failures during boot (often used to hide system changes) Writes data to a remote process
Fingerprint	Queries kernel debugger information Queries process information Reads system information using Windows Management Instrumentation Commandline (WMIC) Reads the active computer name Reads the cryptographic machine GUID Reads the windows installation language
Evasive	Contains ability to detect virtual environment (API) Input file contains API references not part of its Import Address Table (IAT) Marks file for deletion Possibly checks for the presence of an Antivirus engine
Ransomware	Deletes volume snapshots (often used by ransomware) Detected indicator that file is ransomware
Network Behavior	Contacts 48 hosts. View all details