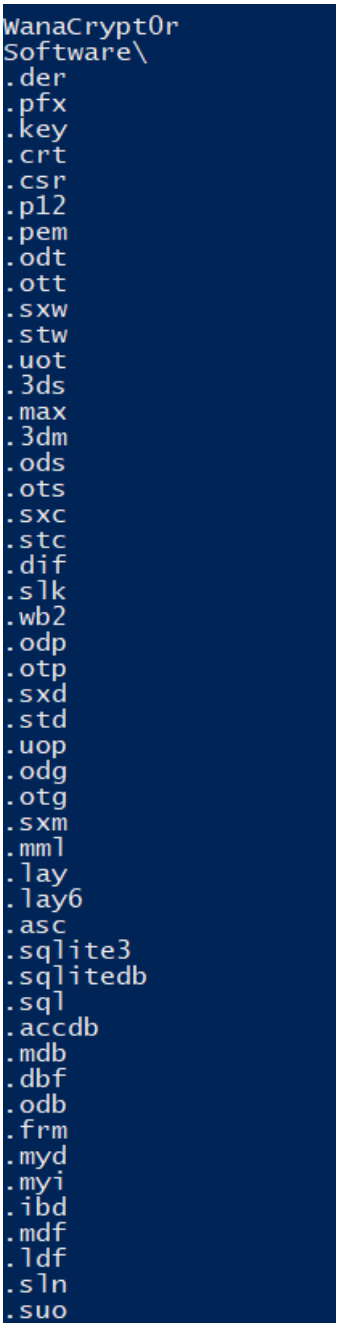
Ciberseguridad: Análisis de malware (C|AM)

Diego Jhosué Cornejo Li

INDICE

1. ¿Que strings importantes encuentras en la muestra?



Hay extensiones de varios tipos de archivos (.sql, xlsx, docx, doc, etc), además del “WannaCrypt0r” que ya indica que el archivo es un malware WannaCry

También contiene rutas como: Intel o ProgramData

Por otro lado también está el “diskpart.exe”, que según he investigado ayuda a administrar las unidades del equipo, pudiendo ser clave en la encriptación de los archivos por el ransomware

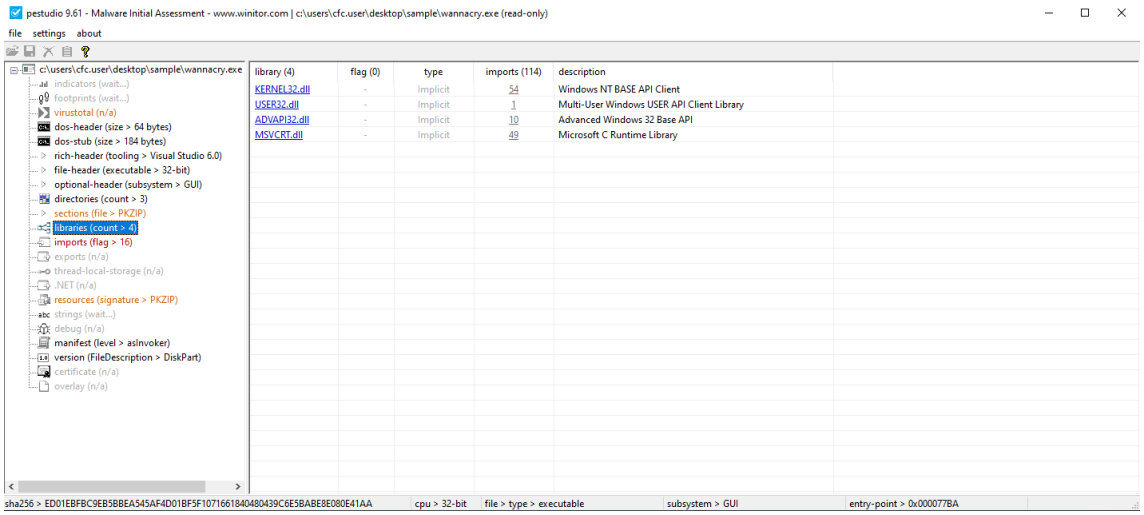
2. Listado completo de .dll llamados por la muestra.

ADVAPI.dll

KERNEL32.dll

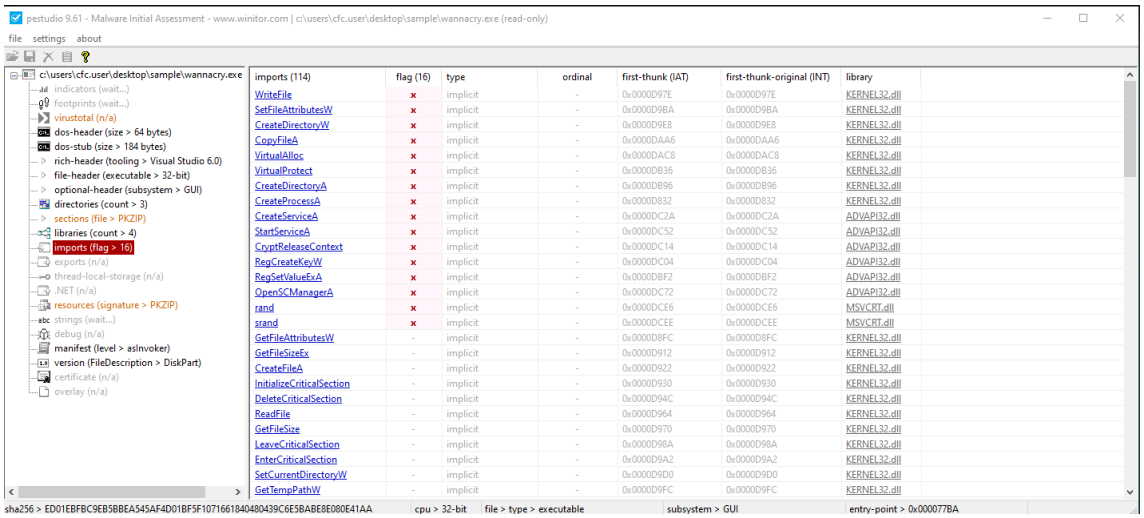
MSVCRT.dll

USER32.dll



3. Listado y explicación de las API que TÚ consideras más importantes para el análisis de la muestra.

API marcadas como flag en pestudio:



- Permite al programa gestionar los archivos del sistema:
    - WriteFile
    - SetFileAttributesW:
    - CopyFileA
    - CreateDirectoryA
    - SetCurrentDirectoryW
- Usado para la persistencia del malware:
    - CreateProcessA
    - CreateServiceA
    - StartServiceA
    - OpenSCManagerA
- Uso de apis para asignar parte de la memoria para el proceso de inyección del malware
    - VirtualAlloc
    - VirtualProtect
- Utiliza APIs criptograficas https://malapi.io/winapi/CryptReleaseContext
    - CryptReleaseContext
- Estas apis generan numeros pseudoaleatorios: https://learn.microsoft.com/en-us/cpp/c-runtime-library/reference/srand?view=msvc-170
    - rand
    - srand

4. Según tu análisis estático, que intuyes que realice el malware al ejecutarlo. Fundamenta tu respuesta

Después de analizar la muestra, por los strings, dlls y apis se puede concluir que el malware es un ransomware.

Por su definición el ransomware es un software que cifra archivos y exige un pago para recuperarlos, usando apis de KERNEL32.dll para poder acceder a archivos del sistema para posteriormente cifrarlos con funciones criptográficas CryptReleaseContext y generación de números pseudoaleatorios (rand, srand) y mantener persistencia en el sistema creando servicios e iniciándolos con CreateService, StartService. Además de apoyarse de memoria para terminar su proceso de inyección de malware.

Este software encriptaría la mayoría de los archivos, por el análisis de strings se vió que hay varias extensiones de archivos comunes como .sql .doxc .xlsl etc.