Guatemala 30 de marzo de 2022

LABORATORIO 4 - Clasificación de Malware

Security Data Science

Luis Alejandro Urbina - 18473
Isabel Ortiz Naranjo - 18176

Análisis Estático

1. Utilice la herramienta pefile para examinar el PE header y obtenga las DLL y las APIs que los ejecutables llaman. ¿Qué diferencias observa entre los ejemplos? ¿Existe algún indicio sospechoso en la cantidad de DLLs y las APIs llamadas?

Los ejecutables tienen en común las llamadas **kernel32.dll**, **msvcrt.dll** y **user32.dll**. kernel32.dll permite acceder a funciones del sistema. El segundo permite la realización de llamadas a redes (acceso a internet). El último permite hacer llamadas por el sistema operativo y sus aplicaciones, como botones, acciones del sistema, entre otros. Estos resultan ser sospechosos puesto que estas llamadas otorgan un control casi total del dispositivo.

En cuanto a diferencias, se puede observar que el primero tiene secciones UPX mientras que el otro tiene secciones TXT.

```
Analizing virus ->  sample_qwrty_dk2
1
Secciones
b'UPX0\x00\x00\x00\x00' 0x1000 0x5000 0
b'UPX1\x00\x00\x00\x00' 0x6000 0x1000 4096
b'.rsrc\x00\x00\x00' 0x7000 0x1000 512


Entries
DLL Calls:
b'KERNEL32.DLL'
Function Calls:
         LoadLibraryA
         ExitProcess
         GetProcAddress
         VirtualProtect
DLL Calls:
b'MSVCRT.dll'
Function Calls:
         atol
DLL Calls:
b'SHELL32.dll'
Function Calls:
         SHChangeNotify
DLL Calls:
b'USER32.dll'
Function Calls:
         LoadStringA
DLL Calls:
b'WS2_32.dll'
Function Calls:
         closesocket


TimeStamp
TimeDateStamp : Thu May 14 17:12:40 2009 UTC
Thu May 14 17:12:40 2009 UTC
1
```

```
Analizing virus ->  sample_vg655_25th.exe
2
Secciones
b'.text\x00\x00\x00' 0x1000 0x69b0 28672
b'.rdata\x00\x00' 0x8000 0x5f70 24576
b'.data\x00\x00\x00' 0xe000 0x1958 8192
b'.rsrc\x00\x00\x00' 0x10000 0x349fa0 3448832


Entries
DLL Calls:
b'KERNEL32.dll'
Function Calls:
         GetFileAttributesW
         GetFileSizeEx
         CreateFileA
         InitializeCriticalSection
         DeleteCriticalSection
         ReadFile
         GetFileSize
         WriteFile
         LeaveCriticalSection
         EnterCriticalSection
         SetFileAttributesW
         SetCurrentDirectoryW
         CreateDirectoryW
         GetTempPathW
         GetWindowsDirectoryW
         GetFileAttributesA
         SizeofResource
         LockResource
         LoadResource
         MultiByteToWideChar
         Sleep
         OpenMutexA
         GetFullPathNameA
         CopyFileA
         GetModuleFileNameA
         VirtualAlloc
         VirtualFree
         FreeLibrary
         HeapAlloc
         GetProcessHeap
         GetModuleHandleA
         SetLastError
         VirtualProtect
         IsBadReadPtr
         HeapFree
```

```
        HeapFree
        SystemTimeToFileTime
        LocalFileTimeToFileTime
        CreateDirectoryA
        GetStartupInfoA
        SetFilePointer
        SetFileTime
        GetComputerNameW
        GetCurrentDirectoryA
        SetCurrentDirectoryA
        GlobalAlloc
        LoadLibraryA
        GetProcAddress
        GlobalFree
        CreateProcessA
        CloseHandle
        WaitForSingleObject
        TerminateProcess
        GetExitCodeProcess
        FindResourceA
DLL Calls:
b'USER32.dll'
Function Calls:
        wsprintfA
DLL Calls:
b'ADVAPI32.dll'
Function Calls:
        CreateServiceA
        OpenServiceA
        StartServiceA
        CloseServiceHandle
        CryptReleaseContext
        RegCreateKeyW
        RegSetValueExA
        RegQueryValueExA
        RegCloseKey
        OpenSCManagerA
DLL Calls:
b'MSVCRT.dll'
Function Calls:
        realloc
        fclose
        fwrite
        fread
        fopen
        sprintf
        rand
        srand
        strcpy
        memset
        strlen
        wcscat
```

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.

(Ver screenshots de arriba), cuando las secciones tienen upx significa que está empaquetado.

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	Categoría	API function calls
1	Search for files to corrupt	
2	Copy/delete files	CloseHandle
3	Get information from files	GetFileSize, GetFileSizeEx
4	Move files	
5	Read/write files	WriteFile, CloseHandle
6	Change files' attributes	

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

```
(env) → lab-4 shasum -a 256 sample_vg655_25th.exe
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa  sample_vg655_25th.exe
(env) → lab-4
```

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

Esta le permite hacer llamados a funciones adicionales a las del kernel, como reiniciar el sistema, crear servicios de windows y modificar el registro de windows.

6. Para el archivo "sample_vg655_25th.exe", ¿cuál es el propósito de la API CryptReleaseContext?
Libera la función del servicio criptográfico del proveedor y el contenedor de llaves, puede ser útil para encriptar archivos.

7. Con la información recopilada hasta el momento, indique para el archivo

““sample_vg655_25th.exe” si es sospechoso o no, y cuál podría ser su propósito.

Si es sospechoso, el archivo contiene DLLs y API Calls que le permiten acceder al sistema (para apagarlo y encenderlo por ejemplo), modificar archivos (y encriptarlos) y hacer llamadas a internet. El propósito puede ser encriptar archivos y tomar a la computadora infectada como rehén a cambio de dinero.

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? ¿En qué consiste este malware?

Submission name:	owo_im_not_ransomware_xd.exe
Size:	3.4MiB
Type:	peexe executable
Mime:	application/x-dosexec
SHA256:	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

Si corresponde, el hash encontrado es el mismo.

El nombre del malware es WannCry.

Este malware de tipo ransomware encripta los archivos del ordenador infectado y luego solicita que el usuario realice un pago para poder desbloquear sus archivos.

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?

Si corresponde, como se puede observar. Los archivos se encuentran encriptados y se le solicita al usuario que pague para poder desencriptarlos.