Análisis de malware

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?**

Para el archivo sample_vg655 se encontró que realiza varias invocaciones al kernel, como se observa en la siguiente figura

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.**
   Significa que UPX se utilizan para empaquetar productos legítimos como malware, ya que es de código abierto y admite múltiples arquitecturas y plataformas. El principal problema para los creadores de malware es que la misma herramienta también utiliza un código de desempaquetado para desempaquetar ejecutables maliciosos.

3.

TABLE 1
MAIN MALICIOUS BEHAVIOUR GROUPS OF API CALL FEATURES

Behaviour	Malware Category	API Function Calls
Behaviour 1	Search Files to Infect	FindClose, FindFirstFile, FindFirstFileEx, FindFirstFileName, TransactedW, FindFirstFileNameW, FindFirstFileTransacted, FindFirstStream, TransactedW, FindFirstStreamW, FindNextFile, FindNextFileNameW, FindNextStreamW, SearchPath.
Behaviour 2	Copy/Delete Files	CloseHandle, CopyFile, CopyFileEx, CopyFileTransacted, CreateFile, CreateFileTransacted, CreateHardLink, CreateHardLink, Transacted, CreateSymbolicLink, CreateSymbolic, LinkTransacted, DeleteFile, DeleteFileTransacted.
Behaviour 3	Get File Information	GetBinaryType, GetCompressed, FileSize, GetCompressedFile, SizeTransacted, GetFileAttributes, GetFileAttributesEx, GetFileAttributes, Transacted, GetFileBandwidth, Reservation, GetFileInformation, ByHandle, GetFileInformation, ByHandleEx, GetFileSize, GetFileSizeEx, GetFileType, GetFinalPathName, ByHandle, GetFullPathName, GetFullPathName, Transacted, GetLongPathName, GetLongPathName, Transacted, GetShortPathName, GetTempFileName, GetTempPath.
Behaviour 4	Move Files	MoveFile, MoveFileEx, MoveFileTransacted, MoveFileWithProgress.
Behaviour 5	Read/Write Files	OpenFile, OpenFileById, ReOpenFile, ReplaceFile, WriteFile, CreateFile, CloseHandle.
Behaviour 6	Change File Attributes	SetFileApisToANSI, SetFileApisToOEM, SetFileAttributes, SetFileAttributesTransacted, SetFileBandwidthReservation, SetFileInformationByHandle, SetFileShortName, SetFileValidData

Estos son los ejemplos que da el paper sobre las apis sospechosas, y para este caso, se pueden clasificar en el comportamiento 1, 2, y 4.

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

```
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
```

5. **Para el archivo "sample_vg655_25th.exe", ¿cuál es el propósito de la DLL ADVAPI32.dll?**
   Es una parte de una biblioteca avanzada de los servicios del API que utiliza APIs numerosos incluyendo muchas llamadas de la seguridad y del registro.

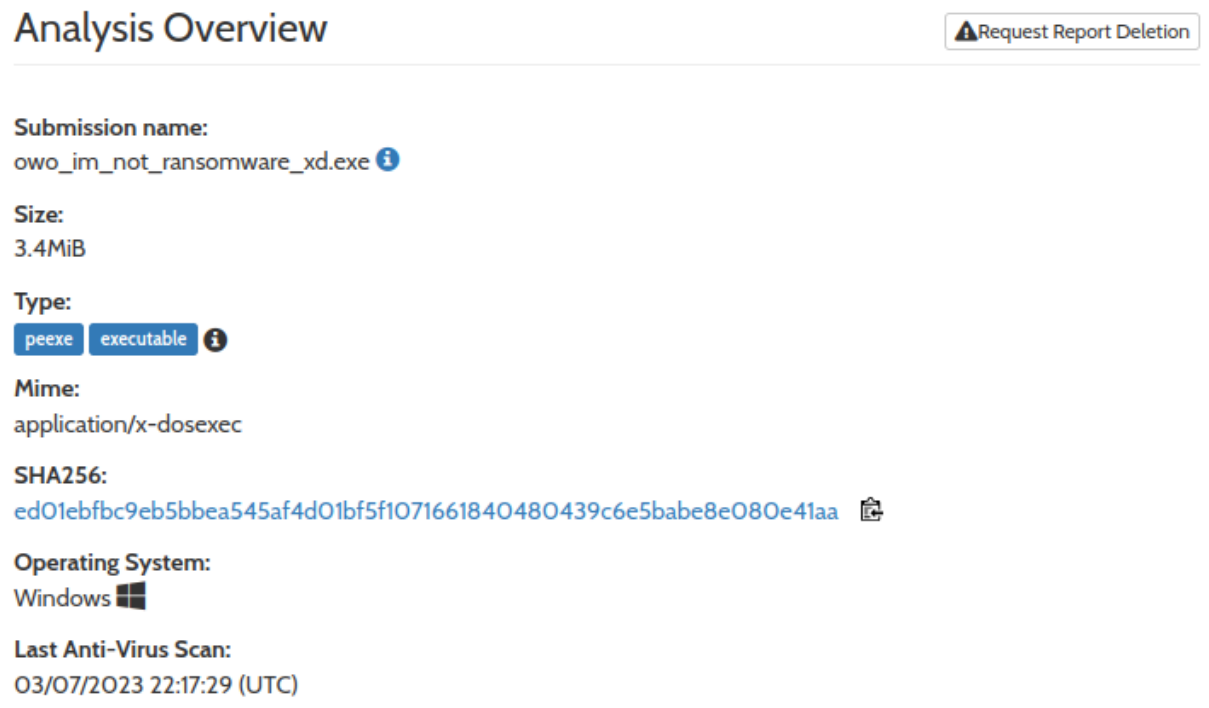
6. **Para el archivo "sample_vg655_25th.exe", ¿cuál es el propósito de la API CryptReleaseContext?**

   El CryptReleaseContext libera el identificador de un proveedor de servicios criptográficos (CSP) y un contenedor de claves.

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 puede considerarse un archivo sospechoso, su propósito podría ser obtener el control e información del dispositivo del usuario.

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?**



Si corresponde el hash con el generado anteriormente. El nombre del malware es owo_im_not_ransomware_xd.exe. Y el propósito es tomar el control del sistema y controlar la información que haya en él.

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?.**

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

Revisando los mensajes de la plataforma, si corresponde a lo que se analizó en el punto 7.