M5-Consegna week 21 day 4 – Daniele Rufo

Ho dato il file a CFF explorer e poi ho interrogato ChatGPT come richiesto per avere info aggiuntive sul malware ed il suo comportamento partendo dai moduli e dalle funzioni importate.

Ecco i moduli:

KERNEL32.dll e SHELL32.dll

Accesso e modifica del file system: i moduli includono funzioni che consentono la creazione di file, la loro cancellazione o la modifica di file di sistema cruciali. Questo è tipico di malware che cercano di installarsi su un sistema o creare file temporanei per eseguire altre attività.

ADVAPI32.dll

Persistenza e modifica del registro di sistema: il malware tenta di modificare il registro di sistema per ottenere persistenza (ad esempio, modificando le chiavi di avvio per avviarsi automaticamente) o per alterare altre configurazioni di sistema a proprio vantaggio.

USER32.dll e GDI32.dll

Intercettazione di input utente: il malware ha capacità di intercettazione degli input utente o di monitoraggio delle finestre. Questa combinazione potrebbe indicare l'uso di keylogger o la cattura di schermate, tecniche tipiche di spyware o trojan.

Quindi ora sappiamo che il malware esegue azioni di basso livello come la creazione di nuovi processi, il controllo di processi in esecuzione o l'allocazione di memoria per iniettare codice dannoso. Queste tecniche sono comuni nei malware che cercano di nascondersi o di eseguire codice arbitrario in altri processi legittimi.

Successivamente ho analizzato le sezioni di cui si compone il malware come segue:

.text - contiene il codice eseguibile del malware. Poiché è contrassegnata come eseguibile e leggibile, possiamo presumere che il codice principale del malware sia contenuto in questa sezione.

.data - contiene dati statici o variabili globali che il malware potrebbe utilizzare durante l'esecuzione. Questa sezione è letta e scritta, ma non contiene codice eseguibile. È tipico che i malware utilizzino questa sezione per conservare dati importanti, come chiavi crittografiche, flag di stato o informazioni temporanee.

.rsrc - contiene le risorse del malware, come icone, stringhe, immagini, o anche dati crittografati o compressi. Nei malware, questa sezione viene talvolta utilizzata per nascondere payload aggiuntivi o dati che verranno successivamente estratti ed eseguiti.

Va sottolineato che l’IA, se interrogata nello specifico sul comportamento del malware consiglia di affiancare un0analisi dinamica a quella statica di base che stiamo effettuando. Il che avvalora la tesi che le tipologie di analisi risultano spesso essere complementari e non sufficienti se isolate.

Grazie