DATA SHIELDS

S10/L1

Maurizio Marcantoni

Traccia

Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L1» presente sul Desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse
- Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa
- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte

Librerie Importate

kernel32.dll

La libreria kernel32.dll è una componente fondamentale del sistema operativo Windows. Il nome "kernel" fa riferimento al nucleo del sistema operativo, che gestisce le operazioni più basse e critiche del sistema. La libreria fornisce l’accesso alle funzioni di base , come la gestione della memoria, la gestione dei file e le operazioni I/O

user32.dll

La libreria user32.dll è un componente cruciale del sistema operativo Windows, responsabile della gestione dell'interfaccia utente. Il suo nome deriva dal fatto che gestisce le funzioni relative all'interazione dell'utente con il sistema operativo.

gdi32.dll

La libreria gdi32.dll è un componente essenziale del sistema operativo Windows che si occupa della grafica. GDI sta per "Graphics Device Interface", e questa libreria è responsabile della gestione delle operazioni grafiche come il disegno di linee, cerchi, testi e la gestione delle immagini.

Sezioni del Malware

.data

é contenente dati inizializzati dal malware. Inludono variabili globali e strutture utilizzate durante l’esecuzione

.text

Questa sezione contiene il codice eseguibile del malware

.rsrc

contiene risorse del programma , icone , immagini , file di dialogo che il malware può utilizzare per presentare interfacce all’utente.

.rdata

contiene dati di sola lettura , come stringhe , puntatorio a funzioni , e altre informazioni di runtime che non vengono modificate durante l’esecuzione

.bss

contiene i dati non inizializzati. questa sezione è utilizzata per variabili globali non inizializzate che vengono impostate a zero all’inizio dell’esecuzione del programma