S10 L01

Davide Andreozzi

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

- KERNEL32.dll
  - contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, gestione della memoria.
- ADVAPI32.dll
  - contiene le funzioni per interagire con i servizi ed i registri del sistema operativo
- MSVCRT.dll
  - contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output.
- WININET.dll
  - contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

Sezioni

- .text
  - Qui sono contenute le istruzioni che la CPU eseguirà a programma avviato. Possiamo definirlo come il cuore del programma
- .rdata
  - Sono incluse le informazioni delle librerie e le funzioni importate ed esportate dall'eseguibile, includono stringhe di testo usate per messaggi di errore o di avviso, tabelle e altri dati che non cambiano durante l'esecuzione del programma. Sono dati in sola lettura e non vengono modificati durante l'esecuzione del programma
- .data
  - Contiene i dati e le variabili globali del programma, globale perché deve è accessibile da qualsiasi funzione

Considerazioni

Le librerie importate indicano che il malware potrebbe utilizzare diverse funzionalità del sistema operativo, come gestione dei processi, comunicazioni di rete e manipolazione dei file. Questo potrebbe indicare un malware complesso.

- Utilizzando la libreria WININET.dll, il malware potrebbe effettuare comunicazioni di rete per inviare dati a un server remoto, ricevere comandi o scaricare ulteriori componenti dannosi.
- Il malware potrebbe cercare di mantenere la sua presenza sul sistema infetto anche dopo il riavvio. Questo potrebbe essere fatto modificando il registro di sistema. Le funzioni della libreria Advapi32.dll potrebbero essere utilizzate per manipolare o creare servizi di sistema nascosti.
- Nella sezione .data possiamo trovare infatti un link che il programma ha memorizzato