S11 L4

Analisi comportamentale delle categorie dei malware più note.

Traccia:

La figura nella slide successiva mostra un estratto del codice di un malware. Identificate:

1. Il tipo di Malware in base alle chiamate di funzione utilizzate.

2. Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa

3. Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo

4. BONUS: Effettuare anche un'analisi basso livello delle singole istruzioni

Il malware è un keylogger che controlla gli input del mouse, questo lo capiamo dalle istruzioni:
push WH_Mouse call
SetWindowsHook()

Le funzioni principali sono:
SetWindowsHook() : Questa funzione installa un hook di procedura in una catena di hook. Il tipo di hook installato dipende dal parametro passato alla funzione. In questo caso, dato che WH_MOUSE è stato spinto nello stack prima della chiamata, SetWindowsHook() installerà un hook del mouse.Il metodo «hook» verrà allertato ogni qualvolta l'utente effettua un click del mouse e salverà le informazioni su un file di log.

CopyFile() : Questa funzione copia un file esistente in un nuovo file. La funzione accetta in input il nome del file esistente, il nome del nuovo file e un parametro che controlla se il nome del nuovo file esiste già, restituisce 0 se la capia fallisce.

mov ecx, [EDI] EDI = «path to startup_folder_system»
mov edx, [ESI] ESI = path_to_Malware
push ecx ; destination folder
push edx ; file to be copied
call CopyFile();

Il malware inserisce all'interno della cartella dei programmi di startup se stesso, così da avviarsi ad ogni startup senza dover modificare eventuali registri.