**FUNZIONALITA’ DEI MALWARE**

Identificare:

**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**

1. Il codice presente nella tabella sotto ci fa pensare ad un Malware di tipo Keylogger, infatti vediamo l’utilizzo della funzione «SetWindowsHook», per l’installazione di un «hook» per controllare un device. Quello che notiamo è che l’ultimo parametro passato sullo stack è «WH\_MOUSE». Questo ci fa pensare che il Malware non registra la digitazione dei tasti della tastiera dell’utente, ma bensì la digitazione dei tasti del mouse

Immagine che contiene testo, schermata, Carattere, numero

Descrizione generata automaticamente

1. Il Malware ottiene la persistenza copiando il suo eseguibile nella cartella di «startup del sistema operativo». Il codice presente nella tabella a partire dall’istruzione 00401040, dapprima setta a zero il registro ECX, successivamente inserisce rispettivamente il path della cartella «startup\_folder\_system» e l’eseguibile del Malware nei registri ECX ed EDX. In seguito, passa entrambi i registri alla funzione CopyFile() con le due istruzioni push ECX e push EDX. La funzione CopyFile() quindi copierà il contenuto di EDX (ovvero l’eseguibile del malware) nella cartella di startup del sistema operativo.

Immagine che contiene testo, schermata, Carattere, bianco

Descrizione generata automaticamente