Traccia:

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

- Il tipo di Malware in base alle chiamate di funzione utilizzate. Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa.
- Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo.
- Effettuare anche un'analisi basso livello delle singole istruzioni.

1. Tipo di malware in base alle chiamate di funzione utilizzate:

- SetWindowsHook(): Questa funzione viene comunemente utilizzata per installare un hook di Windows, in questo caso specifico un hook per il mouse. Questo suggerisce che il malware potrebbe essere un keylogger o un trojan che registra le attività dell'utente.

- CopyFile(): Questa funzione viene utilizzata per copiare un file da una posizione all'altra. Nel contesto del malware, potrebbe essere utilizzata per propagare il malware stesso o per copiare file di configurazione o altri componenti necessari per il funzionamento del malware.

2. Metodo utilizzato per ottenere la persistenza sul sistema operativo:

Il malware utilizza il hook di Windows installato per rimanere attivo e monitorare le attività dell'utente. Questo gli permette di essere eseguito ogni volta che vengono eseguite azioni legate al mouse, garantendo una sorta di persistenza nel sistema.

3. Analisi a basso livello delle singole istruzioni:

- push eax: Salva il valore del registro eax nello stack.

- push ebx: Salva il valore del registro ebx nello stack.

- push WH_Mouse: Salva l'identificatore del tipo di hook (`WH_Mouse`, hook per il mouse) nello stack.

- call SetWindowsHook(): Chiama la funzione SetWindowsHook() per installare il hook di Windows.

- XOR ECX, ECX: Esegue un'operazione di XOR tra il registro ECX e sè stesso, effettivamente azzerandolo.

- mov ecx, [EDI]: Carica il valore dalla memoria all'indirizzo contenuto nel registro EDI nel registro ECX. Questo suggerisce che EDI potrebbe contenere il percorso della cartella di avvio del sistema.

- mov edx, [ESI]: Carica il valore dalla memoria all'indirizzo contenuto nel registro ESI nel registro EDX. Questo suggerisce che ESI potrebbe contenere il percorso del malware.

- push ecx: Salva il contenuto del registro ECX (presumibilmente il percorso della cartella di avvio del sistema) nello stack.

- push edx: Salva il contenuto del registro EDX (presumibilmente il percorso del malware) nello stack.

- call CopyFile(): Chiama la funzione CopyFile() per copiare il file del malware nella cartella di avvio del sistema.