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

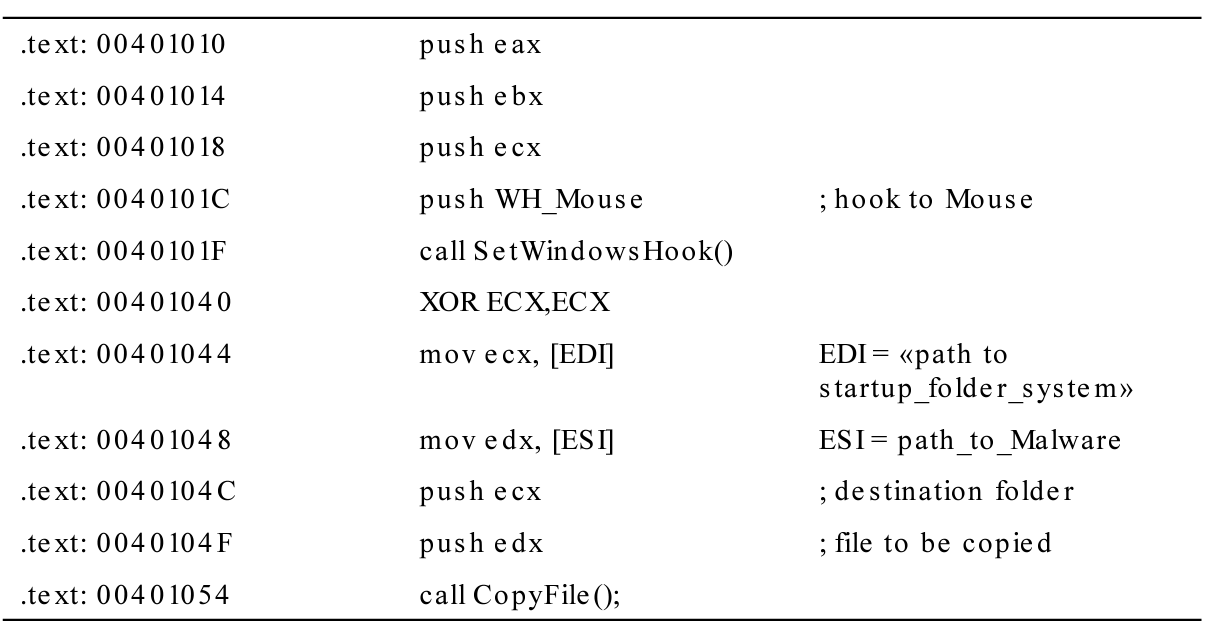
1. Il tipo di Malware in base alle chiamate di funzione utilizzate. Esercizio Funzionalità Malware

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

**SLIDE DI RIFERIMENTO**



**SOLUZIONE**

Alla quinta riga possiamo osservare come venga utilizzata la funzione “**SetWindowsHook**”, ovvero un’API che ha lo scopo di registrare determinati eventi su una macchina; in particolare nella riga sopra (la 4) il programma di debugging evidenzia che si tratta di un “hook to mouse”.

Possiamo, dunque comprendere che si tratta di un **Keylogger** che prende di mira il **mouse** della vittima.

A partire dalla funzione “**004401040**” la funzione utilizza uno XOR per settare a **0** il registro **ECX**; Successivamente vengono passati allo stesso registro ECX i paramentri di cui ha bisogno il malware per funzionare; vediamo di seguito il funzionamento delle righe.

.text:00401044 mov ecx, [EDI] ; EDI = «path to startup\_folder\_system»

Carica nel registro ecx il valore puntato dal registro EDI. Questo valore rappresenta il percorso alla cartella di avvio del sistema.

.text:00401048 mov edx, [ESI] ; ESI = path\_to\_Malware

Carica nel registro edx il valore puntato dal registro ESI. Questo valore rappresenta il percorso al file del malware.

.text:0040104C push ecx ; destination folder

Spinge il valore contenuto nel registro ecx (il percorso alla cartella di destinazione) sullo stack.

.text:0040104F push edx ; file to be copied

Spinge il valore contenuto nel registro edx (il percorso al file del malware) sullo stack.

.text:00401054 call CopyFile()

Chiama la funzione CopyFile per copiare il file del malware (specificato nel registro edx) nella cartella di avvio del sistema (specificata nel registro ecx).

Riassumento, possiamo dire che il malware in questione è un **mouse keylogger**, che invierà ad un server in ascolto le operazioni effettuate dal malware. Il malware tenta di ottenere persistenza replicandosi all’interno dei file di registro di windows, in modo da essere avviato insieme ai file di sistema leggittimi di avvio (e si anniderà in «path to startup\_folder\_system»).