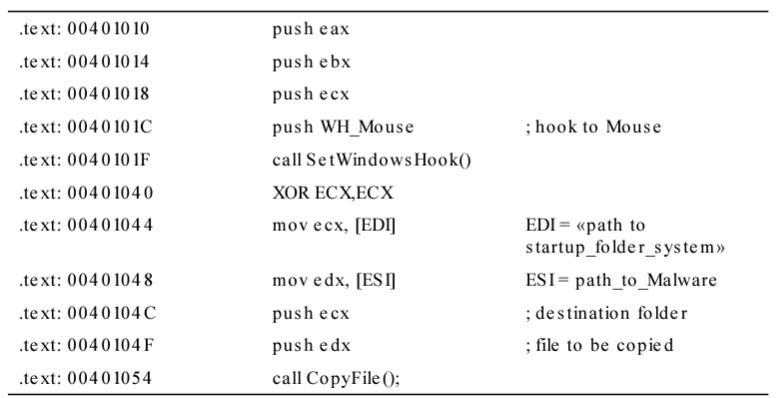
**Malware analysis - Funzionalità dei Malware**

**Traccia:**

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

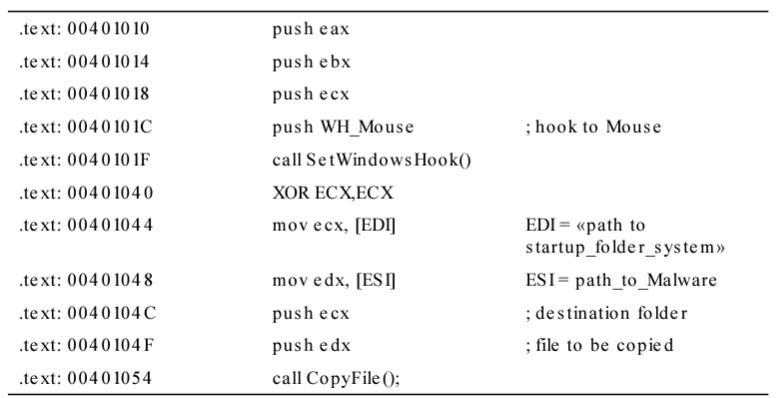
1. Il tipo di Malware in base alle chiamate di funzione utilizzate.
2. Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa
3. Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo **4.** **BONUS:** Effettuare anche un’analisi basso livello delle singole istruzioni



**Svolgimento esercizio:**

# Traccia 1

Dal codice evidenziato in figura è possibile capire che il malware in questione è un keylogger, che rileva i movimenti e i click del mouse della macchina target.

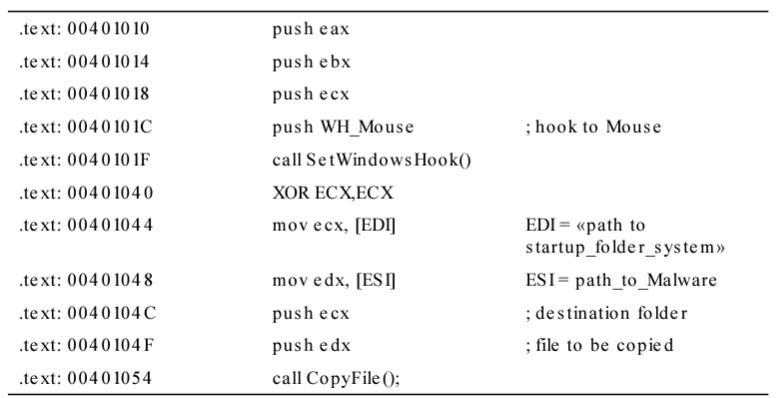


Traccia 2

Le funzioni principali sono:

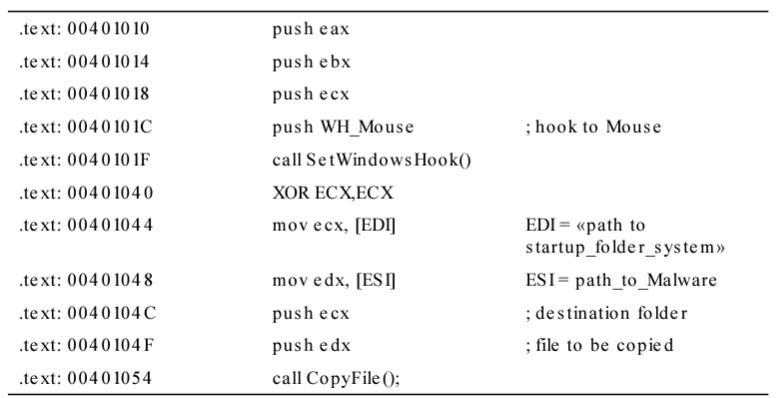
**SetWindowsHook():** questa funzione non fa altro che installare un metodo (una funzione) chiamato «hook» dedicato al monitoraggio degli eventi di una data periferica, come ad esempio la tastiera o il mouse e, successivamente, il metodo «hook» verrà allertato ogni qualvolta l’utente digiterà un tasto sulla tastiera e salverà le informazioni su un file di log.

**CopyFile():** questafunzione di solito fa parte delle API di un sistema operativo, come le Windows API in ambienti Microsoft, che permette il trasferimento di file, dove gli autori di malware molto spesso sfruttano queste funzioni a loro vantaggio per diversi scopi, quali: la raccolta informazioni, la manipolazione dei dati, la possibilità tramite la loro capacità di camuffamento e persistenza, di diffondersi in altri pc copiando se stesso in diverse directory o su dispositivi esterni come USB(tipico comportamento adottato dai worm e dai virus).



**Traccia 3**

Il metodo utilizzato dal malware per ottenere la persistenza sul sistema operativo, lo si può notare guardando attentamente le due righe di codice evidenziate dal rettangolo rosso, dove i valori di EDI ed ESI vengono copiati nei registri ECX e EDX e dove andrà successivamente a scrivere il path del malware direttamente nel path dello startup del sistema. Di conseguenza, questa azione permetterà al malware di avviarsi direttamente all’ avvio del sistema operativo.



**Traccia 4 push eax:** questo inserisce in cima allo stack di memoria il registro eax. **push ebx:** questo inserisce in cima allo stack di memoria il registro ebx. **push ecx:** questo inserisce in cima allo stack di memoria il registro ecx.

**push WH\_Mouse:** questo inserisce in cima allo stack di memoria l’hook WH\_Mouse per aver traccia della periferica mouse.

**call SetWindowsHook:** questo chiama la funzione SetWindowsHook che tiene traccia delle periferiche indicate nella precedente istruzione. **xor ecx, ecx:** l’ operatore logico xor azzera il contenuto del registro ecx. **mov ecx, [EDI]:** copia nel registro ecx il contenuto dell’indirizzo di memoria EDI. **mov edx, [ESI]:** copia nel registro edx il contenuto dell’indirizzo di memoria ESI. **push ecx:** questo inserisce in cima allo stack di memoria il registro ecx. **push edx:** questo inserisce in cima allo stack di memoria il registro edx. **call CopyFile():** chiama la funzione CopyFile.