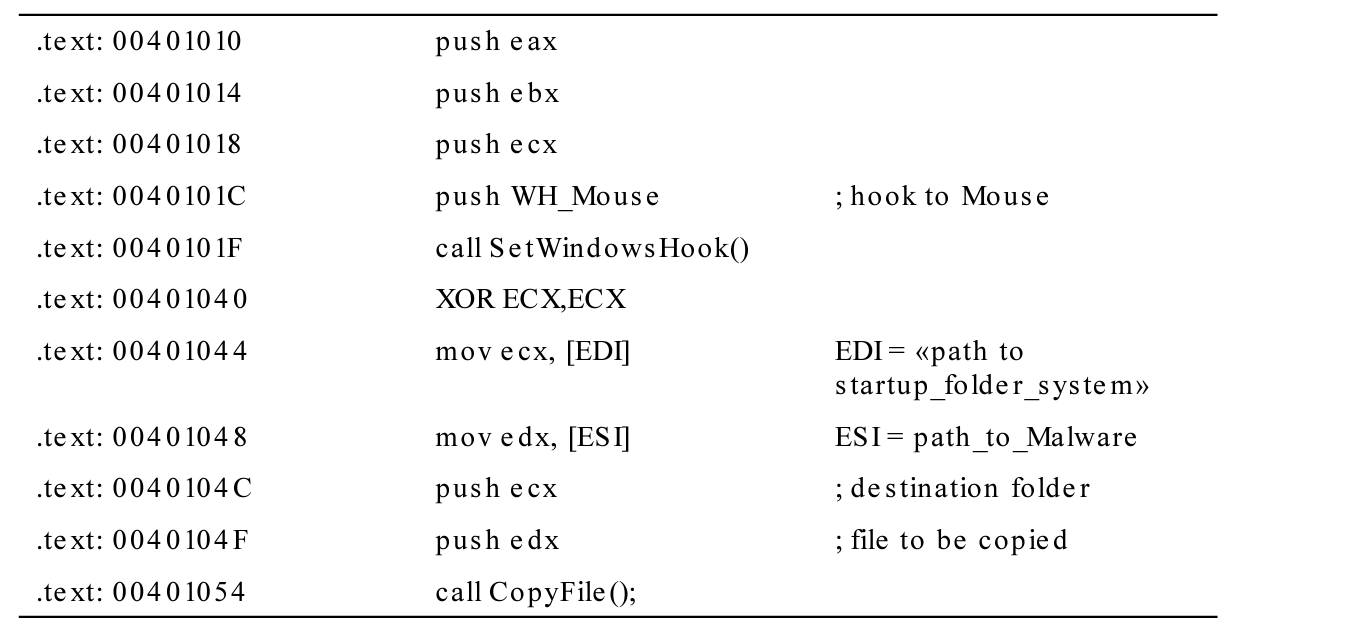
**Funzionalità dei Malware**

Traccia:

La figura 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



**1)** **Tipo di Malware:** In base alle funzioni chiamate, il malware sembra essere un keylogger. L'uso di SetWindowsHook() suggerisce che sta cercando di intercettare input da dispositivo di puntamento (come il mouse), che è tipico dei keylogger.

**2) Chiamate di Funzione Principali**:

* **SetWindowsHook()**: Questa funzione installa un hook che monitora gli eventi di input. Nel contesto del malware, è utilizzata per catturare e registrare l'input dell'utente, in questo caso, movimenti o clic del mouse.
* **CopyFile()**: Questa funzione copia un file da una posizione (ESI) a un'altra (ECX). Nel malware, è utilizzata per duplicare il file malevolo nel sistema, probabilmente per assicurarsi che sia eseguito all'avvio del sistema.

**3)** **Metodo di Persistenza**: Il malware utilizza la cartella di avvio del sistema, indicata come **startup\_folder\_system** (EDI), per copiarsi e quindi eseguirsi ogni volta che il sistema operativo viene avviato. Questo è ottenuto tramite la funzione **CopyFile()**, che copia il file del malware nella cartella di avvio.