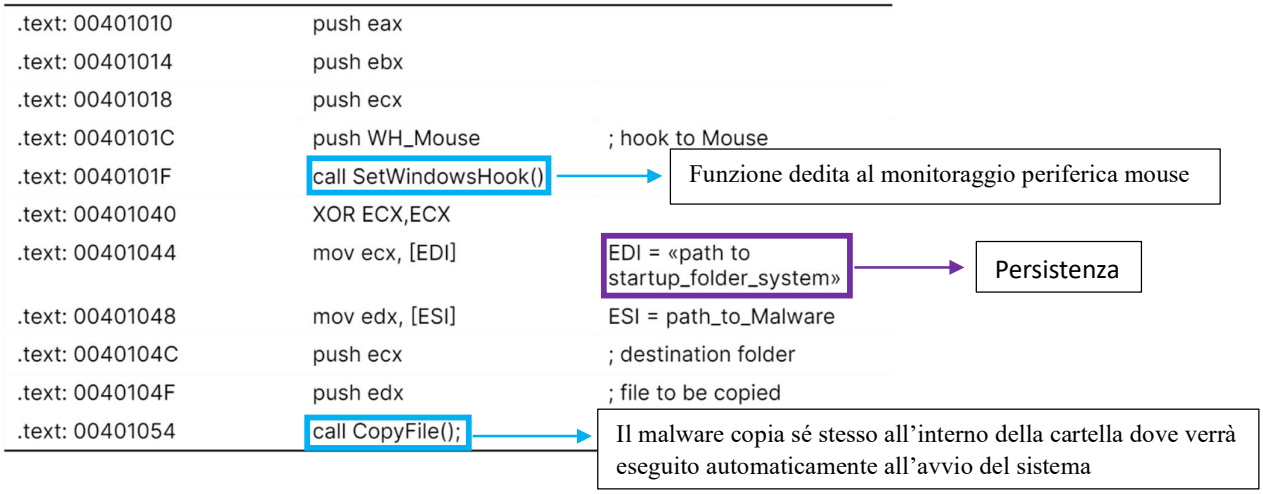
Esercizio Epicode 13/07/2023

Figura 1:



Punto 1:

In base alle chiamate di funzione analizzate, il tipo del malware sembra essere un **Keylogger**, un malware programmato per intercettare tutto ciò che l'utente della macchina infetta digita sulla tastiera al fine di rubare informazioni confidenziali.

Punto 2:

- **SetWindowsHook():** questa chiamata installa una funzione chiamata **hook** dedicata al monitoraggio degli eventi di una data periferica, in questo caso il mouse.
- **CopyFile():** attraverso questa funzione il malware copia il suo file eseguibile all'interno del dispositivo stesso.

Punto 3:

Per ottenere la persistenza, il malware copia sé stesso nella **startup_folder**, una particolare cartella dove i programmi al suo interno vengono eseguiti all'avvio del sistema.

Bonus:

I parametri della funzione vengono pushati sullo stack prima della chiamata alla funzione.

call SetWindowsHook(): la chiamata di funzione

XOR ECX, ECX = 0

mov ecx, [EDI]: copia il contenuto dell'indirizzo di memoria specificato da EDI (path to startup_folder_system) nel registro ecx.

mov edx, [ESI]: copia il contenuto dell'indirizzo di memoria specificato da ESI (path_to_Malware) nel registro edx.

I nuovi parametri della funzione vengono pushati.

call CopyFile(): chiamata di funzione dove il Malware copia il suo eseguibile.