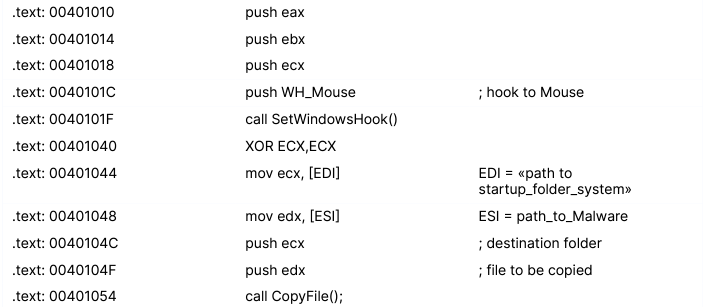
Esercizio 4 settimana 11

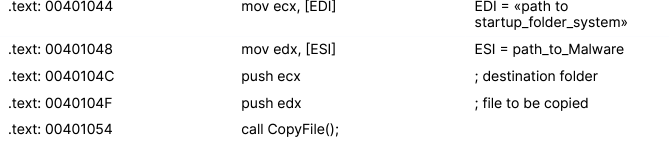
Oggi andremo ad analizzare una porzione di codice assembly per capire di che malware stiamo parlando.



Date queste istruzioni, possiamo comprendere in modo veloce che si tratta di un keylogger, che però non andrà a registrare i tasti premuti sulla tastiera, bensì i click del mouse. Ciò può essere capito da queste istruzioni:



Inoltre, possiamo capire che il malware ottiene persistenza grazie alle seguenti istruzioni:



Come si può capire da queste istruzioni, il malware andrà a inserire il path della cartella “Startup\_Folder\_System” e l’eseguibile del malware stesso nei registri ECX e EDX. Successivamente verrà effettuata una call “Copyfile” in questo modo l’eseguibile verrà salvato nella cartella sopra citata.