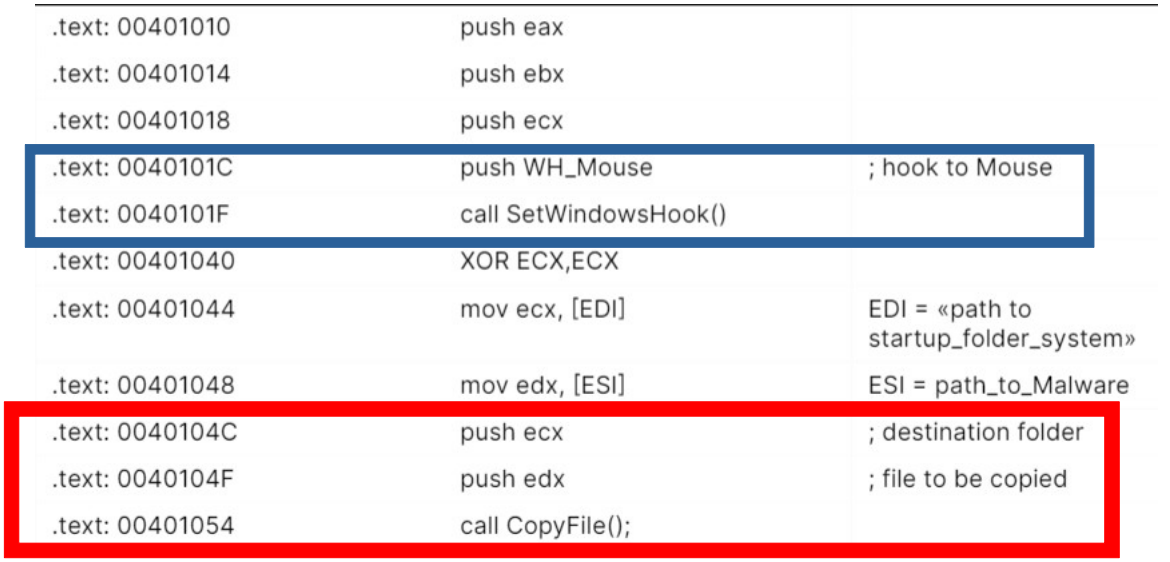
Funzionalità del Malware

La traccia di oggi ci chiedeva di valutare il seguente malware :



.text: 00401010	push eax	
.text: 00401014	push ebx	
.text: 00401018	push ecx	
.text: 0040101C	push WH_Mouse	; hook to Mouse
.text: 0040101F	call SetWindowsHook()	
.text: 00401040	XOR ECX,ECX	
.text: 00401044	mov ecx, [EDI]	EDI = «path to startup_folder_system»
.text: 00401048	mov edx, [ESI]	ESI = path_to_Malware
.text: 0040104C	push ecx	; destination folder
.text: 0040104F	push edx	; file to be copied
.text: 00401054	call CopyFile();	

1) Il tipo di Malware in base alle chiamate di funzione.

Analizzando le righe di codice in particolare : push **WH_Mouse** che andrà a mettere nello stack di memoria ogni input del mouse e con il call **SetWindowsHook** andremo ad associare a gli hook a un thread. Queste righe di codice mi fanno pensare che fino a questo punto questo si tratti di un **keylogger**, in particolare uno che copia le azioni del mouse.
Continuando ad analizzare le righe di codice si può notare come il malware copia con la funzione **Copyfile** il suo percorso dentro la cartella di startup, mettendosi cosi in condizione di avere sia **persistenza** sia l'abilita di avviarsi automaticamente all' avvio del pc.

2) Evidenziare le chiamate di funzione aggiungendo una descrizione per ognuna di esse.

Le funzioni usate dal malware sono riportate di seguito:

call **SetWindowsHook:** Questa funzione monitora gli input di un determinato tipo di eventi che nel nostro caso andrà a monitorare gli eventi del mouse, che poi saranno associati ad un thread.

call **CopyFile:** copia il contenuto di un dato file in un nuovo file. Nel nostro caso questo copierà il path del malware nello stratup_folder_system, mettendosi cosi in condizione di avere sia persistenza sia l'abilita di avviarsi automaticamente all' avvio del pc.

3) Il metodo utilizzato dal Malware per ottenere persistenza sul sistema operativo.

Il malware copia con la funzione **Copyfile** il suo percorso dentro la cartella di startup, mettendosi cosi in condizione di avere sia **persistenza.**

4) BOUNS: Effettuare anche un’ analisi a basso livello per singola istruzione.

Riga di codice	Descrizione
Push eax	Mette nello stack di memoria il registro eax.
Push ebx	Mette nello stack di memoria il registro ebx
Push ecx	Mette nello stack di memoria il registro ecx.
Push WH_Mouse	Mette nello stack di memoria l’ hook del mouse.
Call SetWindowsHook()	La funzione monitora gli eventi del mouse.
XOR ECX,ECX	Con l’ operatore logico XOR mettiamo a zero il valore del registro ECX.
Mov ecx,[EDI]	Spostiamo il contenuto del registro di memoria EDI nel registro ecx.
Mov edx,[ESI]	Spostiamo il contenuto del registro di memoria ESI nel registro edx.
Push eax	Mette nello stack di memoria il registro eax.
Push edx	Mette nello stack di memoria il registro edx.
Call CopyFile()	Copierà il path del malware nello stratup_folder_system.