Gabriele Di giampietro **Esercitazione 19/01/2023**

Obbiettivo: Nell'estratto di codice di un Malware nella figura sotto identificate

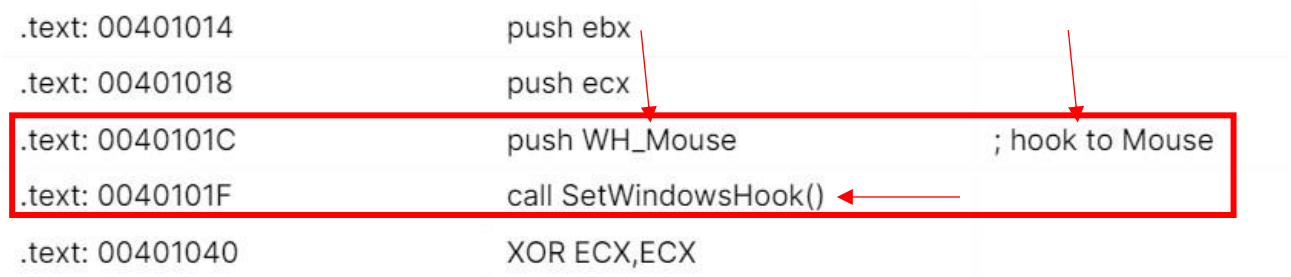
1. Il tipo di Malware in base alle chiamate di funzione utilizzate.
2. Evidenziate le chiamate di funzione principali aggiungendo una **descrizione** per ognuna di essa
3. Il metodo utilizzato dal Malware per ottenere la **persistenza** sul sistema operativo
4. BONUS: Effettuare anche un'analisi basso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

.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();	

Punto 1

Nel primo punto della nostra esercitazione andiamo ad indentificare il tipo di Malware che ci è stato dato, possiamo dedurre abbastanza facilmente che il tipo di Malware che stiamo analizzando sia un **Keylogger** e cioè un programma in grado di intercettare tutto ciò che l'utente digita, prendendo il controllo sia della tastiera che del mouse come nel nostro caso. Infatti possiamo notare che nel codice avviene una chiamata di funzione a **SetWindowsHook( ),** dove questa funzione non fa altro che installare un metodo chiamato **Hook** dedicato al monitoraggio degli eventi di una data periferica, ad esempio tastiera e mouse.

Il metodo Hook verrà allegato ogni volta che l'utente digiterà un tasto sulla tastiera o sul mouse e salverà le informazioni sui file di log.

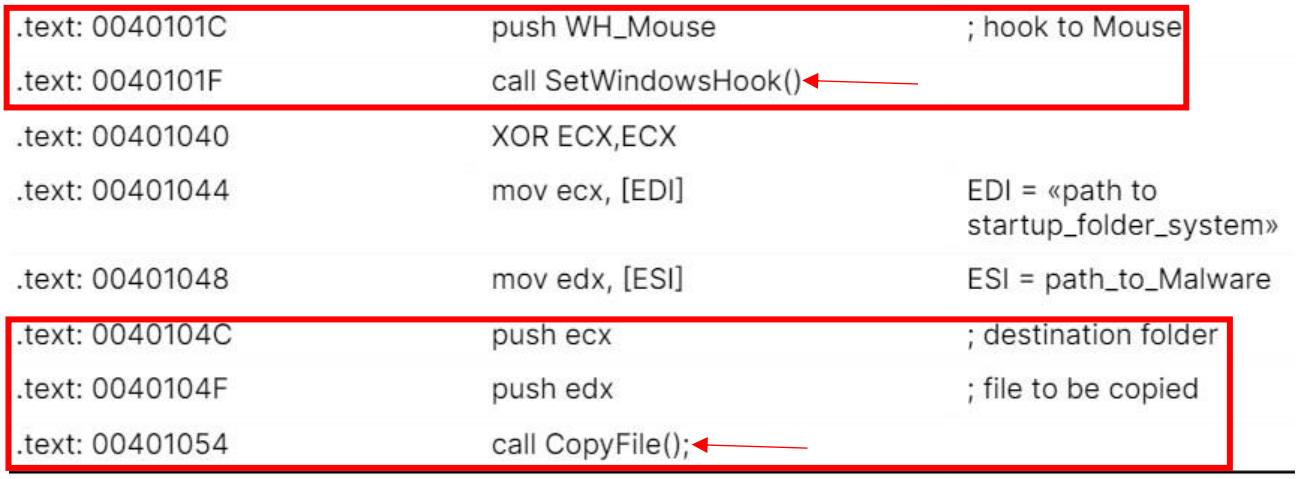


Attraverso l'istruzione Push viene caricato sullo Stak il parametro del controllo del mouse: L'**WH_MOUSE**

hook consente di monitorare i messaggi del mouse, per monitorare l'input pubblicato in una coda di messaggi.

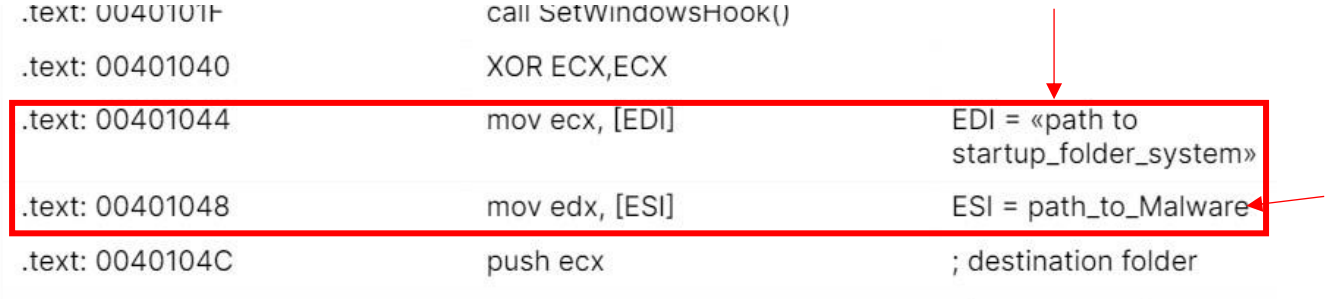
Punto 2

Le principali chiamate di funzione del codice sono 2, una è quella che definisce la tipologia del Malaware che abbiamo visto al punto 1, cioè **SetWindowsHook( ),** e la seconda la troviamo all'ultima riga ed è **CopyFile( ).** Questa funzione Copia uno o più file da una posizione a un'altra. Anche in questo caso i parametri sono inseriti dalle istruzioni Push sopra nello Stak.



Punto 3

Analizzando il codice troviamo anche il punto dove il Malware avvia la sua **Persistenza,** lo troviamo sulle righe dove nel registro EDI corrisponde il path dello **Startup folder system** e sul registro ESI corrisponde il path del Malware. Infatti sappiamo che lo **Startup Folder** è una particolare cartella del sistema operativo che avvia tutti i programmi dell'utente, inserendosi in questa cartella il Malware viene eseguito all'avvio del sistema operativo insieme a tutti i programmi della macchina.



Punto 4 (Bonus)

Nell'ultimo punto andiamo ad effettuare un'analisi a basso livello, cioè diamo una piccola spiegazione delle istruzioni che troviamo nell'estratto di codice.