Progetto **06/04/2023**

Identificazione del Malware

Il codice presente nella tabella in figura ci indica un Malware di tipo Keylogger (programma in esecuzione come processo in background sul computer che registra i tasti premuti dall'utente sulla propria tastiera), infatti vediamo la funzione 'SetWindowsHook', per l'installazione di un 'hook' utilizzata per controllare un device. Si può notare però che l'ultimo parametro passato sullo stack è 'WH_Mouse'. Questo sta a significare che il Malware non registra la digitazione dei tasti della tastiera dell'utente, ma bensì la digitazione dei tasti del mouse:

.text: 00401010	push eax	
.text: 00401014	push ebx	
.text: 00401018	push ecx	
.text: 0040101C	push WH_Mouse	; hook to Mouse
.text: 0040101F	call SetWindowsHook()	

Persistenza del Malware

Il Malware ottiene la persistenza copiando il suo eseguibile nella cartella di startup del sistema operativo. Il codice presente nella tabella a partire dall'istruzione 00401040, dapprima setta a zero il registro **ECX**, successivamente inserisce rispettivamente il path della cartella startup_folder_system e l'eseguibile del Malware nei registri **ECX** ed **EDX**. In seguito, passa entrambi i registri alla funzione CopyFile() con le due istruzioni push ECX e push EDX. La funzione CopyFile() quindi copierà il contenuto di **EDX**, ovvero l'eseguibile del malware, nella cartella di startup del sistema operativo:

.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();	