FUNZIONALITA' DEI MALWARE

TASK:

1. **Identificare il tipo di malware in base alle chiamate di funzione usate**
2. **Evidenziare 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 un'analisi basso livello delle singole istruzioni**

TASK 1: IDENTIFICARE IL TIPO DI MALWARE IN BASE ALLE CHIAMATE DI FUNZIONE USATE

Data la presenza dell'istruzione **push WH_Mousee** e della chiamata di funzione **call SetWindowsHook()**, si può ipotizzare che il malware oggetto d'interesse sia un KEYLOGGER.

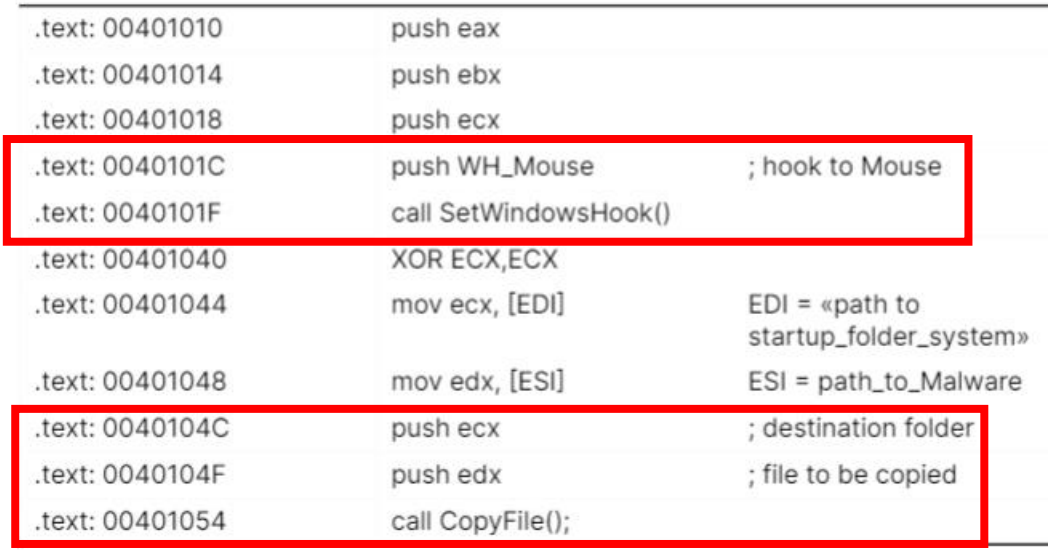
.text: 00401010	push eax	
.text: 00401014	push ebx	
.text: 00401018	push ecx	
.text: 0040101C	push WH_Mouse	; hook to Mouse
.text: 0040101F	call SetWindowsHook()	
.text: 00401040	XOR ECX,ECX	
.text: 00401044	mov ecx, [EDI]	EDI = «path to startup_folder_system»
.text: 00401048	mov edx, [ESI]	ESI = path_to_Malware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

TASK 2: EVIDENZIARE LE CHIAMATE DI FUNZIONE PRINCIPALI, AGGIUNGENDO UNA DESCRIZIONE PER OGNUNA DI ESSA

Si notano due chiamate di funzione principali, **call SetWindowsHook()** e **call CopyFile().**

- **Call SetWindowsHook**() è una funzione che installa un **metodo hook**, **dedicato al monitoraggio degli eventi di una data periferica**, come ad esempio la **tastiera** o il **mouse**. Nel nostro caso, basandoci sull'istruzione **push WH_Mouse**, si nota che il dispositivo in questione è il **mouse**.

- **Call CopyFile()** è una funzione che copia un file esistente in un nuovo file.



.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();	

TASK 3: IL METODO UTILIZZATO DAL MALWARE PER OTTENERE LA PERSISTENZA SUL SISTEMA OPERATIVO

Il metodo utilizzato dal malware oggetto d'interesse per ottenere la persistenza sul sistema operativo è **la sua copia all'interno della cartella Startup_folder_system**, particolare **cartella** del sistema operativo che **viene controllata all'avvio del sistema, ed i programmi che sono al suo interno vengono eseguiti.**

.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();	

TASK BONUS: EFFETTUARE UN'ANALISI BASSO LIVELLO DELLE SINGOLE ISTRUZIONI

1. **Push EAX - Inserisce il valore contenuto nel registro EAX in cima allo stack di memoria.**
2. **Push EBX – Inserisce il valore contenuto nel registro EBX in cima allo stack di memoria.**
3. **Push ECX - Inserisce il valore contenuto nel registro ECX in cima allo stack di memoria.**
4. **Push WH_Mouse - Inserisce l'hook WH_Mouse per il monitoraggio del mouse in cima allo stack di memoria.**
5. **Call SetWindowsHook() - Chiama la funzione SetWindowsHook() per configurare il monitoraggio delle periferica mouse indicata in precedenza.**
6. **XOR ECX, ECX - Azzera il contenuto del registro ECX utilizzando l'operatore logico XOR.**
7. **Mov ECX, [EDI] - Copia il contenuto dell'indirizzo di memoria [EDI] nel registro ECX.**
8. **Mov EDX, [ESI] - Copia il contenuto dell'indirizzo di memoria [ESI] nel registro EDX.**
9. **Push ECX - Inserisci il valore contenuto nel registro ECX in cima allo stack di memoria.**
10. **Push EDX - Inserisce il valore contenuto nel registro EDX in cima allo stack di memoria.**
11. **Call CopyFile() - Chiama la funzione CopyFile() per copiare un file.**