Figura 1:

.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();	

Traccia:

La figura nella slide successiva mostra un estratto del codice di un malware.
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

1. **Tipo di Malware in base alle chiamate di funzione utilizzate**:
   - La chiamata di funzione **SetWindowsHook()** suggerisce che il malware potrebbe essere un keylogger o un tipo di malware che intercetta gli eventi del mouse o della tastiera.
2. **Evidenziazione delle chiamate di funzione principali con descrizioni**:
   - **SetWindowsHook()**: Questa funzione imposta un hook del sistema, che potrebbe essere utilizzato per intercettare e monitorare gli eventi del mouse. Questa funzionalità potrebbe essere impiegata per raccogliere informazioni sull'attività dell'utente.
3. **Metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo**:
   - Il malware sembra ottenere la persistenza copiandosi nella cartella di avvio del sistema. Le istruzioni **mov ecx, [EDI]** e **mov edx, [ESI]** caricano rispettivamente i percorsi per la cartella di avvio del sistema e per il malware nei registri **ecx** e **edx**. Successivamente, i valori di **ecx** e **edx** vengono spinti nello stack con le istruzioni **push ecx** e **push edx**. Questi valori nello stack sono probabilmente

passati come argomenti per una funzione che copierà il malware nella cartella di avvio del sistema.

4. **Analisi basso livello delle singole istruzioni**:
    - Le istruzioni **pusheax**, **pushebx**, **pushecx** mettono i valori dei registri **eax**, **ebx**, e **ecx** nello stack per conservarli.
    - **push WH_Mouse** mette l'identificatore **WH_Mouse** nello stack come argomento per la chiamata di funzione successiva.
    - **call SetWindowsHook()** chiama la funzione **SetWindowsHook()** per impostare un hook del sistema.
    - **XOR ECX, ECX** esegue un'operazione XOR tra il registro **ecx** e se stesso, azzerandolo.
    - **mov ecx, [EDI]** e **mov edx, [ESI]** caricano rispettivamente i percorsi per la cartella di avvio del sistema e per il malware nei registri **ecx** e **edx**.
    - Le istruzioni **push ecx** e **push edx** mettono i valori dei registri **ecx** e **edx** nello stack, presumibilmente come argomenti per una chiamata di funzione successiva