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.) SI tratta di un keylogger con la funzionalità di ottenere persistenza. Lo vediamo dalla funzione **SetWindowsHook()** che si tratta di un keylogger.

2.) Infatti le funzioni principali chiamate sono 2: la prima appunto è quella che identifica il tipo di malware ovvero il keylogger. Infatti la funzione SetWindowsHook() usa come parametro WH_Mouse, quindi viene passato tramite l'istruzione push sullo stack un hook (un meccanismo attraverso il quale intercettare eventi) per monitorare input del mouse. L'altra chiamata di funzione è **CopyFile().** Questa funzione serve per poter copiare il file dell'eseguibile(del malware) all'interno di una delle cartelle **startup_folder** in modo da ottenere la persistenza.

3.) Il malware per ottenere la persistenza usa la tecnica della <<startup_folder>> ovvero cerca di copiare il proprio file eseguibile all'interno di una di queste cartelle. Ricordiamo che il S.O windows mantiene due tipi di cartelle (una generica e una dedicata agli utenti) di startup_folder che vengono controllate all'avvio del pc e i programmi al loro interno di conseguenza vengono eseguiti. Se l'attaccante riesce a copiare l'eseguibile dentro una di queste 2 cartelle, viene eseguito il malware all'avvio del pc.

4.) BONUS:

- La prima istruzione aggiunge il registro EAX allo stack tramite istruzione push e viene fatta la stessa cosa con i registri EBX, ECX

- Viene poi passato sullo stack il parametro WH_Mouse della funzione **SetWindowsHook()** sempre tramite l'istruzione push. Per cui si va ad intercettare gli input del mouse in risposta a dei messaggi.
- Successivamente viene invocata la funzione sopracitata.
- Si inizializza a 0 il registro ECX tramite lo XOR.
- Avendo inizializzato a 0 il registro ECX, viene in seguito copiato in tale registro il path della <<startup_folder>> contenuto nell'indirizzo di memoria del registro EDI tramite l'istruzione MOV
- Viene copiato nel registro EDX il valore contenuto nell'indirizzo di memoria del registro ESI, ovvero il path del malware.
- Vengono aggiunte allo stack quindi il registro ECX (che praticamente contiene la destinazione in cui deve essere copiato il file eseguibile) e il registro EDX (che di fatto contiene il file eseguibile da copiare)
- Infine viene chiamata la funzione per copiare il file eseguibile nella cartella di destinazione <<startup_folder>>