Esercizio S11L4

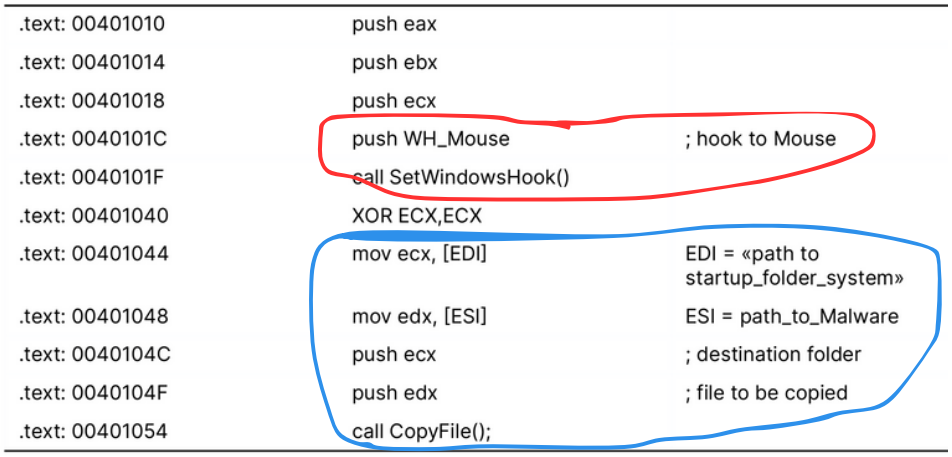
Traccia:

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

- Il tipo di Malware in base alle chiamate di funzione utilizzate. Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa
- Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo

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();	



Keylogger

Persistenza

Il malware in questione è un **keylogger** nello specifico un keylogger che utilizza **SetWindowsHookEx()** che fa parte di una delle due macrocategorie.

Questa funzione, **SetWindowsHookEx()**, non fa altro che installare un metodo (una funzione) chiamato «hook» dedicato al monitoraggio degli eventi di una data periferica, come in questo caso il mouse. Il metodo «hook» verrà allertato ogni qualvolta l'utente farà un movimento o dell'azioni con il mouse(esempio: clic, doppio clic, trascinamenti, rilasci, ecc.) e salverà le informazioni su un file di log.

Nella funzione **CopyFile()** il malware quando identifica il dispositivo esterno, copia se stesso (il suo file eseguibile) all'interno del dispositivo stesso.

Persistenza: il malware aggiunge sé stesso nei programmi che devono essere avviati all'avvio del PC in modo tale da essere eseguiti in maniera automatica e permanente senza l'azione dell'utente. Metodo utilizzato dal malware è il startup folder

Startup folder è uno dei metodi di persistenza che prevede di copiare il suo eseguibile in una delle cartelle di startup (che sia la cartella dedicata ad un utente specifico oppure la cartella di startup comune a tutti gli utenti)