ESERCIZIO 4 SETTIMANA 11

1)Il codice che stiamo analizzando sembra indicare la presenza di un possibile malware di tipo keylogger. Questo perché vediamo l'utilizzo della funzione "SetWindowsHook" per installare un "hook" che monitora un dispositivo. Tuttavia, notiamo una differenza rispetto al codice della lezione teorica: l'ultimo parametro passato è "WH_MOUSE". Questo suggerisce che il malware potrebbe non registrare la pressione dei tasti sulla tastiera dell'utente, ma piuttosto la movimentazione 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()	

2)Il malware ottiene la persistenza copiando il suo eseguibile nella cartella di avvio del sistema operativo. Il codice presente nella tabella inizia impostando a zero il registro ECX e poi inserisce il percorso della cartella di avvio del sistema operativo e il nome dell'eseguibile del malware nei registri ECX ed EDX rispettivamente. Successivamente, passa entrambi i registri alla funzione CopyFile() utilizzando le istruzioni push ECX e push EDX. Questo fa sì che la funzione CopyFile() copi il contenuto di EDX (cioè l'eseguibile del malware) nella cartella di avvio del sistema operativo.

.text: 00401044	mov ecx, [EDI]	EDI = «startup_folder_system»
.text: 00401048	mov edx, [ESI]	ESI = Malware_name
.text: 0040104C	push ecx	; destination folder
.text: 0040104F	push edx	; file name
.text: 00401054	call CopyFile();	