Pratica S11/L4

Il codice suggerisce la presenza di un possibile malware tipo keylogger, focalizzato sulla registrazione dei clic del mouse anziché della tastiera. Per rimanere persistente nel sistema operativo, il malware copia il suo eseguibile nella cartella di avvio. Il codice sembra mirare a registrare attività del mouse e a mantenere una presenza duratura nel sistema.

.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();	