

## PRATICA S11L4

Analizzando il codice proposto, il malware sembra essere di tipo keylogger. Andiamo ad analizzare le funzioni implementate:

.text: 00401010	push eax	
.text: 00401014	push ebx	
.text: 00401018	push ecx	
.text: 0040101C	push WH_Mouse	; hook to Mouse
.text: 0040101F	call SetWindowsHook()	

In questa sezione vengono passati sullo stack gli argomenti della funzione SetWindowsHook(). Questa funzione serve a registrare gli input immessi dall'utente. In particolare vediamo che viene passato il WH\_Mouse, quindi una volta chiamata la funzione verranno registrati i movimenti e gli input dati dall'utente tramite mouse

.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();	

In questa sezione il malware cerca di ottenere persistenza sul sistema. Il metodo utilizzato è quello di copiare il file malware all'interno della cartella di startup del sistema operativo, attraverso la funzione CopyFile(). Sullo stack vengono passati come argomenti il percorso alla cartella di startup e il percorso del malware.