.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();	

- In base alle funzioni utilizzate dal malware possiamo dedurre che appartenga alla tipologia "keylogger" poichè utilizza la funzione "SetWindowsHook" per l installazione di una procedura "hook" per controllare un device.

Il parametro "WH_MOUSE" passato sullo stack ci fa dedurre che il malware registra la digitazione dei tasti del mouse.

La funzione CopyFile copia il contenuto di edx nella cartella di startup del sistema operativo

- Per ottenere la permanenza nel sistema vittima, il malware effettua una copia di se stesso nella cartella di startup