

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

vengono dichiarate le variabili e chiamate le funzioni WH\_Mouse che registra gli input del mouse e SetWindowsHook che registra gli input da tastiera.

.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

Viene azzerato il valore di ECX

Viene poi spostato [EDI] in ECX e [ESI] in EDX

Qui viene creata la persistenza all'avvio

.text: 0040104C	push ecx	; destination folder
.text: 0040104F	push edx	; file to be copied
.text: 00401054	call CopyFile();	

E qui viene richiamata la funzione principale

Il malware analizzato è un Keylogger