Analisi dinamica avanzata

.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();	

Queste linee di codice evidenziano che il malware al primo utilizzo del mouse, eseguirà tramite la funzione una registrazione di tutti gli input che vengono mandati dalla periferica.

Il metodo che il malware usa per la persistenza sono le linee di codice:
push WH_Mouse
call SetWindowsHook().