La chiamata alla funzione che possiamo subito notare in questo codice è "SetWindowsHook()". Questa funzione viene usata per creare un "hook", ovvero una funzione che serve a monitorare costantemente una determinata periferica di un dispositivo, in questo caso il mouse (lo si può notare da WH_Mouse).
Questo è l'indizio che potrebbe trattarsi di un Keylogger.

Il modo in cui il malware mantiene la persistenza nel sistema operativo, invece, è tramite lo "Startup_folder", nel comando "mov ecx, [EDI]". Questo fa sì che, all'avvio del dispositivo, il malware sia già in funzione, pronto a tener traccia degli input dati dal mouse sfruttando la cartella di startup di windows.

I dati in input verranno poi salvati su un file di log.

```
.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();
```