Funzionalità dei malware

andiamo ad analizzare il seguente codice

```
.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();
```

all'interno di questo codice possiamo notare che è un logger del mouse

```
.text: 0040101C    push WH_Mouse              ; hook to Mouse
.text: 0040101F    call SetWindowsHook()
```

notiamo che prende persistenza andando a immettersi nella path dello startup del sistema operativo

```
.text: 00401044    mov ecx, [EDI]             EDI = «path to
                                              startup_folder_system»
.text: 00401048    mov edx, [ESI]             ESI = path_to_Malware
```

inoltre notiamo come ultima funzione la copia del file

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

nel analisi di basso livello del codice vediamo le funzioni come seguono
mette il registro eax in cime alla pila
mette ebx in cima alla pila
mette ecx in cima alla pila
mette il WH_mouse in cima alla pila
chiama la funzione setwindowshook()
resetta ecx al valore 0
mette la “strada” per raggiungere la cartella di startup del sistema operativo nel registro ecx
mette la “strada” per il malware nel registro edx
mette ecx in cima alla pila
mette edx in cima alla pila

chiama la funzione copia file