Funzionalità malware

Sull'estratto del codice che segue, rispondi alle seguenti domande:

.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();	

1) **Il tipo di malware in base alle chiamate di funzione utilizzate.**
   In base alle funzioni chiamate, il malware è un **keylogger**. Le funzioni chiamate sono: **SetWindowsHook() e CopyFile().**

2) **Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa.**
   Nell' estratto di codice viene chiamata la funzione **SetWindowsHook(),** funzione che installa un metodo chiamato **hook** , dedicato al monitoraggio degli eventi di una periferica come ad esempio la tastiera o il mouse. In questo caso monitora il **mouse**, infatti come parametro viene pushato **WH_Mouse**. La funzione **CopyFile** copia edx (percorso del malware) nella cartella ecx (percorso cartella startup).

3) **Identificare il metodo utilizzato dal malware per ottenere la persistenza sul sistema operativo.**
   La persistenza viene ottenuta copiando il file del malware nella cartella di startup di sistema, così il malware si avvia automaticamente ogni volta che il sistema operativo viene avviato.

4) **Effettua un'analisi di basso livello delle singole istruzioni.**

```
push eax
push ebx
push ecx
```

Viene inizializzato lo stack, pushando i 3 registri al suo interno.

```
push WH_Mouse      ; hook to Mouse
call SetWindowsHook()
```

Il valore Wh_Mouse viene salvato nello stack, parametro utilizzato dalla funzione SetWindowsHook.

```
XOR ECX ,ECX
```

Con lo XOR viene azzerato il registro di ECX.

```
mov ecx, [EDI]              ; EDI = <<path to startup_folder_system>>
mov edx, [ESI]              ; ESI = path_to_Malware
```

Vengono copiati i percorsi nei registri ecx ed edx.

```
push ecx                    ; cartella di destinazione
push edx                    ; file da copiare
```

Vengono salvati i parametri sullo stack per la funzione CopyFile()

```
Call CopyFile()
```

Esegue la copia del file