Funzionalità dei malware

1. L'analisi del codice presente nella tabella suggerisce la presenza di un potenziale malware di tipo keylogger. Questa conclusione deriva dall'utilizzo della funzione "SetWindowsHook" per installare un "hook", finalizzato al monitoraggio di un dispositivo. È da notare che l'ultimo parametro passato sullo stack è "WH_MOUSE", indicando che il malware potrebbe registrare l'input proveniente dai movimenti del mouse.

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

2. Il malware ottiene la persistenza nel sistema operativo copiando il suo file eseguibile nella cartella di avvio automatico del sistema.
   Il codice nella tabella, a partire dall'istruzione 00401040, inizia azzerando il registro ECX, poi inserisce il percorso della cartella "startup_folder_system" e l'eseguibile del malware nei registri ECX ed EDX. Successivamente, entrambi i registri vengono passati alla funzione CopyFile() tramite le istruzioni push ECX e push EDX.
   La funzione CopyFile() procederà quindi a copiare il contenuto di EDX, ossia l'eseguibile del malware, nella cartella di avvio automatico del sistema operativo.

```
.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();
```