```
.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. Tipo di Malware:

Le chiamate di funzione principali nel codice includono:

‘SetWindowsHook()’: Questa funzione viene utilizzata per installare un hook di Windows. Nel codice fornito, viene utilizzato per installare un hook per intercettare gli eventi del mouse. Questo suggerisce che il malware potrebbe essere un keylogger o un programma che monitora l'input dell'utente, poiché intercetta gli eventi del mouse.
‘CopyFile()’: Questa funzione viene utilizzata per copiare un file da una posizione all'altra. Nel codice fornito, il malware copia se stesso in una directory specifica, suggerendo che cerca di ottenere la persistenza sul sistema operativo copiando se stesso nella cartella di avvio del sistema.

2. Metodo di Persistenza:

Il malware utilizza la funzione ‘CopyFile()’ per copiare se stesso in una directory specifica. Questo suggerisce che il malware cerca di ottenere la persistenza sul sistema operativo copiando se stesso nella cartella di avvio del sistema, in modo che venga eseguito automaticamente ogni volta che il sistema si avvia. La directory specificata potrebbe essere la cartella di avvio del sistema operativo, come "Startup" o "Startup Programs", indicata dalla variabile ‘EDI’ nel codice fornito, che rappresenta il percorso della cartella di avvio del sistema.