Funzioni Principali

Le prime istruzioni push inseriscono i registri eax, ebx, ecx e il valore WH_Mouse nello stack, seguite dalla chiamata SetWindowsHook(), che permette di installare hooks per intercettare i messaggi di input del mouse, della tastiera, della finestra e di altri eventi di sistema. In questo caso WH_Mouse indica che l'hook deve intercettare i messaggi di input 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()
```

L'istruzione XOR ECX,ECX imposta il registro ecx a zero.

```
XOR ECX,ECX
```

Persistenza

Le istruzioni mov ecx, [EDI] e mov edx, [ESI] caricano rispettivamente nei registri ecx e edx i valori contenuti negli indirizzi di memoria, che sono rispettivamente la cartella di avvio del sistema operativo e il malware.

```
EDI = «startup_folder_system»
ESI = Malware_name
```

Le istruzioni push ecx e push edx inseriscono i valori dei registri ecx e edx nello stack.

L'istruzione call CopyFile() chiama la funzione di sistema CopyFile(), che copia il malware nella cartella di avvio.

```
push ecx          ; destination folder
push edx          ; file name
call CopyFile();
```

In questo modo il malware viene eseguito automaticamente ad ogni avvio del sistema.

Spiegazione Malware

Il malware con la funzione SetWindowsHook() installa un hook di sistema per intercettare i click del mouse. Con la funzione CopyFile() copia il malware nella cartella di avvio del sistema operativo, in modo che il malware venga eseguito automaticamente ad ogni avvio del sistema.