| | | |
|---|---|---|
| .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(); | |

In base alle chiamate di funzione utilizzate, il malware mostrato nell'immagine è un trojan. I trojan sono un tipo di malware che si presenta come un software legittimo, ma in realtà ha lo scopo di infettare il sistema operativo con codice dannoso.

Le chiamate di funzione principali sono le seguenti:

- SetWindowsHook(): questa funzione viene utilizzata per installare un hook sul sistema operativo. Un hook è un programma che viene eseguito ogni volta che si verifica un evento specifico, come ad esempio un clic del mouse. In questo caso, l'hook viene installato per monitorare i clic del mouse;
- CopyFile(): questa funzione viene utilizzata per copiare un file da una posizione ad un'altra. In questo caso, il malware copia se stesso nella cartella di avvio del sistema operativo.

Il malware ottiene la persistenza sul sistema operativo copiando se stesso nella cartella di avvio. In questo modo, esso viene eseguito automaticamente ogni volta che il sistema operativo viene avviato.

La prima chiamata di funzione, SetWindowsHook(), viene utilizzata per installare un hook sul sistema operativo al fine di monitorare i clic del mouse. L'hook viene installato con il parametro WH_Mouse, il quale indica che l'hook verrà eseguito ogni volta che si verifica un evento del mouse.
La seconda chiamata di funzione, CopyFile(), viene utilizzata per copiare il malware nella cartella di avvio del sistema operativo. La posizione della

cartella di avvio viene memorizzata nella variabile EDI. Il malware viene copiato nella cartella di avvio utilizzando il parametro start_up_folder_system.
In conclusione, il malware è un trojan che ottiene la persistenza sul sistema operativo copiando se stesso nella cartella di avvio.