FUNZIONALITÀ DEI MALWARE

Cyber Security & Ethical Hacking

TRACCIA

```
.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();
```

Traccia:

1. Il tipo di Malware in base alle chiamate di funzione utilizzate.

2. Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa

3. Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo

1
Tipo di Malware:

Il malware sembra essere interessato ad installare un hook del mouse e copiare un file in una determinata posizione. Tuttavia, il tipo di malware specifico non può essere identificato in modo preciso solo da queste chiamate di funzione.

2 Chiamate di Funzione Principali:

1. **SetWindowsHook**: Questa funzione viene utilizzata per installare un hook del mouse (**WH_Mouse**). Gli hooks sono spesso utilizzati per monitorare o intercettare eventi di sistema come l'input utente. Nel contesto del malware, potrebbe essere utilizzato per registrare attività del mouse, come il keylogging.
2. **XOR ECX,ECX**: Questa istruzione effettua un'operazione di XOR sul registro ECX con se stesso, azzerandolo. Questo potrebbe essere utilizzato per inizializzare o reimpostare il registro ECX a zero.
3. **movecx, [EDI]**: Sembrerebbe essere un errore di sintassi, probabilmente dovrebbe essere **mov ecx, [EDI]**. Questo carica il contenuto della memoria all'indirizzo specificato da EDI nel registro ECX. In questo caso, EDI contiene il percorso alla cartella di avvio del sistema.
4. **movedx, [ESI]**: Ancora un possibile errore di sintassi, probabilmente dovrebbe essere **mov edx, [ESI]**. Questo carica il contenuto della memoria all'indirizzo specificato da ESI nel registro EDX. In questo caso, ESI contiene il percorso al malware.
5. **pushecx e pushedx**: Queste istruzioni inseriscono i valori dei registri ECX ed EDX nello stack. Questi valori potrebbero essere utilizzati come parametri per una successiva chiamata di funzione.

3 Metodo di Persistenza:

La presenza di un hook del mouse e l'uso di un'operazione di copia dei file (**CopyFile** potrebbe essere utilizzato, ma non è presente nel codice) potrebbero suggerire che il malware possa cercare di inserire se stesso in una posizione persistente nel sistema, ad esempio nel folder di avvio del sistema (**Startup**).