Aprile 2024

CYBER SECURITY SPECIALIST

S11L4

Jacopo Trovato

Funzionalità dei Malware

```
.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();
```

Analizzando Il malware in figura si può vedere che si tratta di un "**Keylogger**", un tipo di software o hardware progettato per registrare e memorizzare ogni pressione di tasti effettuata su una tastiera di un computer, senza il consenso dell'utente. Si può capire vedendo la stringa con la funzione "**callSetWindowsHook**()" e con la stringa "**push WH_Mouse**" viene indicato che il malware monitora i movimenti del mouse.

```
push WH_Mouse          ; hook to Mouse
call SetWindowsHook()
```

```
mov ecx, [EDI]         EDI = «path to
                       startup_folder_system»
mov edx, [ESI]         ESI = path_to_Malware
push ecx               ; destination folder
push edx               ; file to be copied
```

La persistenza viene analizzata grazie a "**startup_folder-system**", e alla stringa "**call Copyfile** ()" questo garantisce l'attivazione malware all'avvio della macchina.

Le chiamate di funzione di questo malware sono:

- call SetWindowsHook() = installare un "hook" di sistema o di processo, che permette di intercettare e monitorare eventi specifici generati dal sistema operativo o da una particolare applicazione.
- call Copyfile () = copia un file da una posizione a un'altra sul sistema operativo Windows. Consente di duplicare un file, creando una copia identica del file originale in un'altra posizione.