Funzionalità dei malware

S11L4

Indice

Traccia

La figura nella slide successiva mostra un estratto del codice di un malware.
Identificate:

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
4. BONUS: Effettuare anche un'analisi basso livello delle singole istruzioni

Traccia

Figura 1:

```
.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();
```

Le funzioni del Malware

Come evidenziato in figura questo malware sembra che faccia una chiamata alla funzione SetWindowsHook che permette di creare un hook (gancio) per copiare tutto ciò che viene cliccato con il Mouse.

```
.text: 00401018    push ecx
.text: 0040101C    push WH_Mouse          ;hook to Mouse
.text: 0040101F    call SetWindowsHook()
.text: 00401040    XOR ECX,ECX
```

Le funzioni del Malware

Come evidenziato in figura il malware si avvia in modo automatico all'avvio del sistema grazie al comando "mov ecx, [EDI]" che è il "path" dello startup system. Grazie ad esso ottiene la persistenza.

```
.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();
```

Bonus

Comando	Descrizione
Push eax	Importa il valore di eax sullo stack
Push ebx	Importa il valore di ebx sullo stack
Push ecx	Importa il valore di ecx sullo stack
Push WH_Mouse	Importa sullo stack il valore della costante WH_Mouse
Call SetWindowsHook()	Fa la chiamata alla funzione SetWindowsHook

Bonus

Comando	Descrizione
XOR ECX, ECX	Inizializza a zero il registro ECX
mov ecx, [EDI]	Inserisce sul registro ecx il path allo startup file system
mov edx, [ESI]	Inserisce sul registro edx il path al maware
push ecx	importa il valore della cartella di destinazione
push edx	importa il valore del file che deve essere copiato
call CopyFile()	chiama la funzione CopyFile

Grazie