S11/L4

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

```
.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();
```

1.Tipo di Malware:
Basandoci sulle chiamate di funzione utilizzate, questo malware sembra essere un tipo di malware che mira a ottenere persistenza sul sistema operativo e potenzialmente anche ad eseguire azioni dannose tramite l'intercettazione degli eventi del mouse.

2.Chiamate di funzione principali:

```
.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();
```

SetWindowsHook(WH_Mouse, ...): Questa chiamata di funzione imposta un hook per intercettare gli eventi del mouse nel sistema operativo. Questo potrebbe essere un passaggio importante per il malware per monitorare l'input del mouse per scopi dannosi.
CopyFile(destination_folder, file_to_be_copied): Questa chiamata di funzione copia un file in un'altra posizione specificata. Il malware sembra utilizzare questa chiamata per copiare se stesso in una cartella di avvio del sistema operativo, garantendo così la persistenza.

3.Metodo per ottenere la persistenza sul sistema operativo:
Il malware ottiene la persistenza copiando se stesso in una cartella di avvio del sistema operativo. Utilizza la funzione CopyFile() per copiare il proprio file eseguibile in una posizione definita (destination folder), che sembra essere la cartella di avvio (path to startup_folder_system). Questo assicura che il malware venga eseguito automaticamente ogni volta che il sistema operativo viene avviato.

4.Analisi basso livello delle istruzioni:

Istruzione	Descrizione
push eax	Mette il valore del registro eax nello stack.
push ebx	Mette il valore del registro ebx nello stack.
push ecx	Mette il valore del registro ecx nello stack.
push WH_Mouse	Mette il valore della costante WH_Mouse nello stack.
call SetWindowsHook()	Chiama la funzione SetWindowsHook() per impostare l'hook per l'intercettazione degli eventi del mouse.
XOR ECX,ECX	Esegue un'operazione XOR sul registro ecx, impostandolo a zero.
mov ecx, [EDI]	Muove il contenuto del puntatore EDI nel registro ecx.
mov edx, [ESI]	Muove il contenuto del puntatore ESI nel registro edx.
push ecx	Mette il valore del registro ecx nello stack.
push edx	Mette il valore del registro edx nello stack.
call CopyFile()	Chiama la funzione CopyFile() per copiare il malware in una nuova posizione nel sistema operativo.