FUNZIONALITÀ DEI MALWARE

S11/L4

ELEONORA VIOLA

TABLE OF CONTENT

INTRODUCTION

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

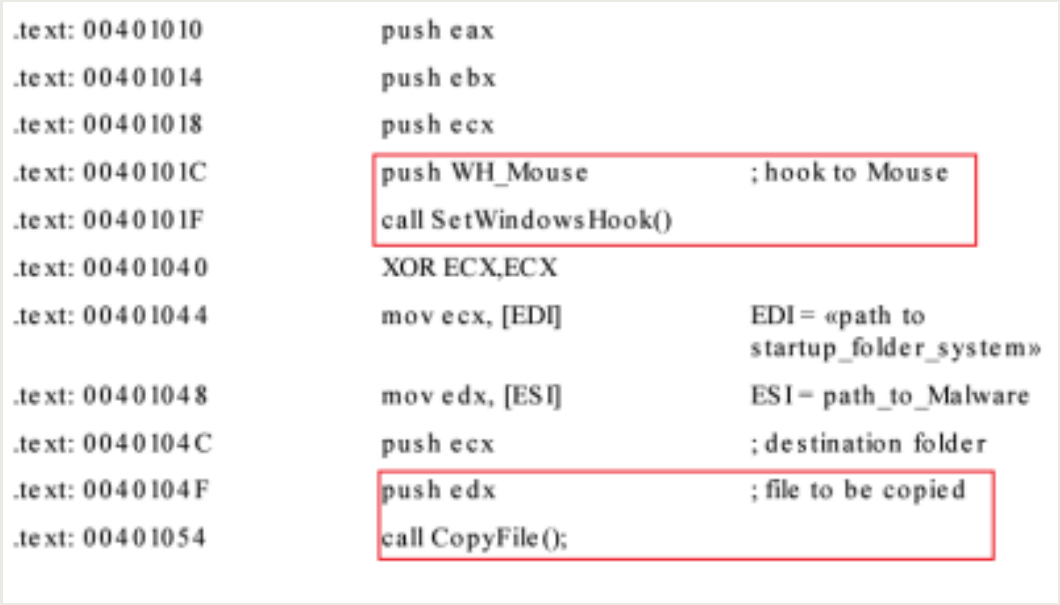
```
.text: 00401010    push eax
.text: 00401014    push ebx
.text: 00401018    push ecx
.text: 0040101C    push WH_Mouse          ; hook to Mouse
.text: 0040101F    call SetWindowsHook()
.text: 00401040    XOR ECX,ECX
.text: 00401044    mov ecx, [EDI]         EDI = «path to
                                          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();
```

PROCEDURE

1.**Task:**

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 e della tastiera (keylogger).

2. Task



.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.

PROCEDURE

3. Task

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. Task

- **push eax, ebx, ecx** — Carica il contenuto di questi registri nello stack;
- **push MH_Mouse** — Carica MH_Mouse nello stack. Questo parametro ci servirà dopo (in SetWindowsHook);
- **call SetWindowsHook** — questa funzione permette di monitorare il sistema per determinati tipi di eventi.
- **xor ecx ecx** — Poichè compara un registro a se stesso è come se stesse pulendo (azzerando) il registro
- **mov ecx, [EDI]** — Sposta il valore dell'indirizzo EDI nel registro ecx
- **mov edx [ESI]** — Sposta il valore dell'indirizzo ESI nel registro edx
- **push ecx edx** — carichiamo i due valori nello stack
- **call CopyFile** — Spiegata nella task 2