Pratica 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 di basso livello delle singole funzioni

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

È un **KEYLOGGER**, un particolare tipo di malware programmato per intercettare tutto ciò che viene digitato sulla tastiera o dall'uso del mouse.

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

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

WH_Mouse: monitora le coordinate globali del movimento del mouse.
SetWindowsHook: Funzione che monitora gli eventi di una periferica.

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

```
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
call CopyFile();
```

Il metodo utilizzato è la «**startup folder**», una particolare cartella dell'OS che viene controllata all'avvio del sistema, eseguendo i programmi al suo interno.
Le cartelle di statup sono:

- Quelle dedicate agli utenti
- Quella generica del Sistema Operativo.

Se il malware riesce a copiare il suo eseguibile all'interno di una delle due cartelle, verrà eseguito automaticamente all'avvio del sistema (**cartella generica**), o all'avvio del sistema del singolo utente (**cartella utente**)

BONUS: Effettuare un'analisi di basso livello delle singole funzioni

push eax
Salva il valore di eax sullo stack

push ebx
Salva il valore di ebx sullo stack

push ecx
Salva il valore di ecx sullo stack

push WH_Mouse ; hook to Mouse
Passa sullo stack l'istruzione WH_Mouse

call SetWindowsHook()
Chiama la funzione SetWindowsHook per monitorare l'uso del mouse

XOR ECX,ECX
Operatore logico che inizializza a 0 il registro

mov ecx, [EDI] EDI = «path to startup_folder_system»
Copia il percorso di EDI in ecx, ovvero la cartella di destinazione generica del Sistema Operativo

mov edx, [ESI] ESI = path_to_Malware
Copia il percorso di ESI in edx, ovvero il percorso da cui copiare il malware

push ecx ; destination folder
Salva la cartella in ecx

push edx ; file to be copied
Salva la cartella in edx

call CopyFile();
Chiama la funzione CopyFile, copiando il malware all'interno della cartella generica del Sistema Operativo