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

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();	

Il tipo di Malware in base alle chiamate di funzione utilizzate
Il malware è un *keylogger* che traccerà i movimenti del mouse sulla macchina e ne creerà un file.

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

Questa funzione non fa altro che installare una funzione chiamata «hook» dedicata al monitoraggio degli eventi di una data periferica, nel nostro caso il mouse

.text: 0040101F call SetWindowsHook()

Questa funzione copia un file già esistente in un nuovo file

.text: 00401054 call CopyFile();

Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo
Il malware va ad inserirsi nel nel file System di windows, precisamente nel *startup_folder_system*

.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

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

- **00401010: push eax** Mette il valore del registro eax nello stack
- **00401014:** push ebx Mette il valore del registro ebx nello stack
- **00401018:** push ecx Mette il valore del registro ecx nello stack
- **40101C:** push WH_Mouse Mette sullo stack un valore (probabilmente una costante o variabile) denominato WH_Mouse. Il commento suggerisce l'intenzione di agganciarsi al mouse
- **0040101F:** call SetWindowsHook() Chiama la funzione SetWindowsHook per impostare un hook di Windows, probabilmente legato agli eventi del mouse
- **00401040:** XOR ECX, ECX Esegue un'operazione XOR sul registro ecx, impostandolo effettivamente a zero
- **401044:** mov ecx, [EDI] Sposta il valore all'indirizzo di memoria puntato da EDI nel registro ecx. Il commento indica che EDI contiene il "percorso alla cartella di avvio del sistema"
- **00401048:** mov edx, [ES1] Sposta il valore all'indirizzo di memoria puntato da ES1 nel registro edx. Il commento indica che ES1 contiene il "percorso a _Malware"
- **0040104C:** push ecx Mette sullo stack il valore di ecx (percorso alla cartella di avvio del sistema)
- **0040104F:** push edx Mette sullo stack il valore di edx (percorso a _Malware)
- **00401054:** call CopyFile() Chiama la funzione CopyFile. Questa funzione è utilizzata per copiare un file esistente in un nuovo file