Esercizio S11 L4

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

- Il tipo di Malware in base alle chiamate di funzione utilizzate. Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa.
- Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo.

.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();	

Tipo di Malware

In base alle chiamate di funzione utilizzate, il malware in questione è un **keylogger.** I keylogger sono malware che registrano la pressione dei tasti da parte dell'utente.

Chiamate di funzione principali

Le chiamate di funzione principali del codice sono le seguenti:

1. **SetWindowsHook()**: Questa funzione viene utilizzata per installare un hook sul sistema operativo. Un hook è un meccanismo che consente al malware di intercettare eventi di sistema, come il click del mouse o la pressione dei tasti. In questo caso, il malware installa un hook sul mouse, in modo da poter registrare le pressioni dei tasti.
2. **CopyFile()**: Questa funzione viene utilizzata per copiare un file da una posizione a un'altra. In questo caso, il malware copia se stesso nella cartella di avvio del sistema operativo.

```
.text: 00401010        push eax
.text: 00401014        push ebx
.text: 00401018        push ecx
.text: 0040101C        push WH_Mouse                ; hook to Mouse
.text: 0040101F    1   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    2   call CopyFile();
```

Metodo di persistenza

Il malware ottiene la persistenza sul sistema operativo copiando se stesso nella cartella di avvio. Questo significa che il malware verrà eseguito automaticamente ogni volta che l'utente avvia il computer.