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

1= Il tipo di malware è un hook in questo caso del mouse, sostanzialmente riesce a recepire i movimenti ed i click del mouse di un utente vittima, successivamente salva un file di testo (che verrà continuamente aggiornato) con tutti i movimenti del mouse.

2=

.text: 0040101C	push WH_Mouse	; hook to Mouse
.text: 0040101F	call SetWindowsHook()	

Questa prima chiamata serve per settare e per far partire l'hook del mouse.

.text: 0040104F	push edx	; file to be copied
.text: 00401054	call CopyFile();	

Questa seconda chiamata permette al malware di salvare tutti i dati recepiti dall'hook su un file di testo.

3=

.text: 00401044	mov ecx, [EDI]	EDI = «path to startup_folder_system»

Il metodo di persistenza utilizzato dal malware è il seguente.