PRATICA S11_L4

Funzionalità dei Malware

La figura nella slide successiva mostra un estratto del codice di un malware, identificare:

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

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();	

SOLUZIONE:

1) In base alle chiamate di funzioni utilizzate si può evincere che si tratta di un Keylogger. Le funzioni principali sono “SetWindowsHook” che monitora gli eventi delle periferiche (in questo caso parliamo del mouse), allertando l’utente ad ogni utilizzo dello stesso, ed anche “CopyFile” utilizzato per copiare file.

2) Per ottenere la persistenza sul sistema operativo il malware copia il suo eseguibile dentro la directory “startup_folder_system” per essere runnato all’avvio del sistema operativo.