PRATICA S11/L4 – Giorgio Trovesi

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();	

- **Identificazione tipo di Malware:**

Possiamo constatare dal codice che il malware utilizza la funzione “SetWindowsHook” per l’installazione di un hook per il controllo di un device, si può presupporre che si tratti del mouse perché viene passato sullo stack il parametro “WH_mouse” e quindi ipotizzare che si tratti di un Keylogger che registra i movimenti del mouse da parte dell’utente.

- **Chiamate di funzione e relativa descrizione:**

SetWindowsHook(): la funzione di hooking in Windows permette di monitorare e intercettare eventi di una periferica come gli input di tastiere e mouse, in questo caso si tratta di un mouse.

CopyFile(): la funzione viene utilizzata per copiare un file da un dato percorso a uno di destinazione, in questo caso sembra copiare se stesso in una cartella del sistema di avvio al fine di ottenere la persistenza.

- **Metodo utilizzato dal malware per ottenere la persistenza:**

Il Malware, come detto in precedenza, cerca di ottenere la persistenza copiandosi in una cartella di avvio; si può vedere che il malware utilizza la funzione CopyFile() per effettuare questa operazione. Il percorso di origine è “path_to_Malware” è contenuto nella variabile ESI mentre quello di destinazione “path to startup_folder_system) è contenuto nella variabile EDI.