Pratica S11/L4 Analisi comportamentale delle categorie dei malware più note

L'esercizio di oggi consiste nell'identificare:

-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

Di questo frammento di codice:

.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 malware utilizza la funzione SetWindowsHook per l'installazione di un hook per il controllo di un device e possiamo notare come viene passato il parametro WH_Mouse quindi possiamo dedurre che sia un keylogger che registra la digitazione del mouse dell'utente collegato alla macchina vittima.

Le chiamate di funzione utulizzate sono 2:

SetWindowsHook(): è una API di Windows che consente di installare un hook di sistema o di applicazione, cioè un punto di monitoraggio per determinati tipi di eventi del sistema operativo o dell'applicazione.

CopyFile(): è una API di Windows utilizzata per copiare un file da una posizione a un'altra nel sistema di file.

Il metodo utilizzato dal malware per ottenere la persistenza sul sistema operativo è tentando di copiarsi in una cartella di avvio utilizzando la funzione di CopyFile().

Il percorso da copiare (path_to_Malware) è contenuto nella variabile ESI, invece il percorso di destino della copia (path to startup_folder_system) è contenuto in EDI.

Infine la funzione CopyFile viene chiamata con questi due percorsi così da garantire l'esecuzione del malware all'avvio della macchina.