Analisi Comportamentale

Malware

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

Le seguenti enunciati:

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();	

- Il tipo di Malware in base alle chiamate di funzione utilizzate:

  Il Malware in particolare è un keylogger, possiamo identificarlo
  Dalla dicitura “hook to Mouse”

- Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa:

  Le funzioni principali del keylogger sono il monitoraggio e la trasmissione di tutto ciò che viene digitato tramite mouse e tastiera, possiamo individuare la sua funzione sotto la dicitura:" call SetWindowsHook()"

- Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo:

  Il metodo utilizzato dal Malware per ottenere la persistenza è copiarsi su una cartella dedicata ad un utente comune tramite lo start up folder

BONUS: Effettuare anche un'analisi basso livello delle singole istruzioni

Nella prima parte del codice il Malware risulta essere un keylogger che si "aggancia" e traccia l'uso del mouse e della tastiera.

La seconda parte del codice si riferiscono al tipo di famiglia del keylogger e l'ultima parte mostra il suo metodo di persistenza