Esercitazione W24D1 - Pratica 2

Funzionalità dei malware

Fabio Benevento - 17/04/2024

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
- Effettuare anche un'analisi basso livello delle singole istruzioni

.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();	

Svolgimento

1) Il malware è di tipo Keylogger, ovvero una tipologia di malware che acquisisce le azioni dell'utente tramite tastiera e mouse. In questo caso infatti viene chiamata la funzione SetWindowsHook con il parametro WH_Mouse, al fine di impostare un handler agli eventi del mouse.

2) Per ottenere la persistenza, il malware copia se stesso (il file) nella cartella di startup di sistema. In questo modo, il malware viene fatto partire ad ogni avvio del sistema

3) Analizzando il codice è possibile evidenziare le chiamate SetWindowsHook() e CopyFile(). Il passaggio dei parametri avviene mediante lo stack.
Per quanto riguarda la SetWindowsHook() questa prende principalmente come parametro il tipo di hook da monitorare, nel caso in esame WH_Mouse per gli eventi del mouse.
La funzione CopyFile() invece prevede come parametri il path alla cartella di startup di sistema (destinazione) e il path a quella del malware (sorgente).