Esercitazione WEEK W24D1 (2)

Funzionalità dei Malware

Ettore Farris

Descrizione sintetica e risoluzione

Traccia:

La figura seguente 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*

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();	

Svolgimento e analisi

Tipo di malware

Il codice effettua una chiamata alla funzione *SetWindowsHook(),* una funzione di sviluppo di Windows che consente di installare un *hook.* In questo caso, prima della call viene *pushato* nello stack il parametro l'*hook WH_MOUSE.* Questo *hook* consente di monitorare i monitorare e intercettare gli eventi del mouse. Possiamo concludere che il malware è uno ***Spyware*** dato che traccia i movimenti del mouse dell'utente.

Persistenza

Successivamente, il malware chiama la funzione *CopyFile(),* che è utilizzata per copiare un file da una posizione a un'altra. Prende come argomenti il percorso del file da copiare e il percorso di destinazione. In questo caso, lo *Spyware* (cioè il file da copiare) viene spostato nella cartella di **esecuzione automatica** in modo che sia persistente e possa essere avviato all'avvio di Windows, resistendo pertanto ai reboot di sistema. Prima di chiamare la funzione:

- Azzera il registro ECX e successivamente vi inserisce il percorso della cartella di esecuzione automatica (contenuto in EDI) tramite l'istruzione MOV ECX, [EDI];
- Nel registro EDX viene passato il path del nostro malware (contenuto in ESI) tramite l'istruzione MOV EDX, [ESI];
- I due registri vengono *pushati* sullo stack e passati come parametri della funzione *CopyFile().*