Malware analysis- Funzionalità dei Malware

Sommario

Traccia S11-L4

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

1. Il tipo di Malware in base alle chiamate di funzione utilizzate.
2. Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa
3. Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo
4. BONUS: 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();	

Analisi del codice

.text: 00401010 push eax **// Pusha il valore corrente del registro eax nello stack**

.text: 00401014 push ebx **// Pusha il valore corrente del registro ebx nello stack**

.text: 00401018 push ecx **// Pusha il valore corrente del registro ecx nello stack**

.text: 0040101C push WH_Mouse ; hook to mouse **// Inserisce l'hook del mouse nello stack**

.text: 0040101F call SetWindowsHook() **// Chiama la funzione SetWindowsHook() per impostare l'hook del mouse**

.text: 00401040 XOR ECX,ECX **// la funzione XOR contenuta inizializza il registro a 0, siccome il risultato di uno XOR tra due operandi uguali è sempre 0.**

.text: 00401044 mov ecx, [EDI] EDI = “path to startup_folder_system” **// Copia il valore dalla posizione di memoria puntata da EDI nel registro ecx. EDI contiene un percorso verso una cartella di avvio del sistema**

.text: 00401048 mov edx, [ESI] ESI = patch_to_malware **// Copia il valore dalla posizione di memoria puntata da ESI nel registro edx. ESI contiene un percorso verso il malware**

.text: 0040104C push ecx ; destination folder **// Inserisce il valore del registro ecx (cartella di destinazione) nello stack**

.text: 0040104F push edx ; file to be copied **// Inserisce il valore del registro edx (file da copiare) nello stack**

.text: 00401054 call CopyFile() **// Chiama la funzione CopyFile() per copiare il file**

Che tipo di malware è?

Il malware analizzato sembra essere un keylogger che monitora le attività relative mouse, come i movimenti e clic.

Come ottiene la persistenza?

Il malware sembra ottenere la persistenza copiandosi nella cartella di avvio del sistema. Questo significa che il malware verrà eseguito ogni volta che il sistema viene avviato

Quali chiamate di funzione utilizza?

1. La funzione SetWindowsHook() è una funzione di Windows che installa una procedura di hook definita dall’applicazione in una catena di hook. Questa funzione è utilizzata per monitorare il sistema per determinati tipi di eventi. In questo caso monitora gli eventi del mouse perché viene pushato nello stack l’hook del mouse.
2. La funzione CopyFile() è una funzione di Windows che copia un file esistente in un nuovo file.