S11/L4 Esercizio 07/12/2023

Nell'esercizio odierno ci viene richiesto di identificare sull'estratto di un codice malware:

- Il tipo di malware in base alle chiamate di funzione utilizzate e di evidenziare le chiamate di funzione principali aggiungendone una descrizione
- Il metodo utilizzato dal malware per ottenere la persistenza sul sistema operativo

Estratto del codice malware

.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();	

Quesito 1

Come possiamo vedere dalle righe di codice **evidenziate in blu** Il tipo di malware utilizzato sembra un **keylogger** e sembra riferirsi al **monitoraggio del mouse**, quindi probabilmente progettato per raccogliere informazioni sull'utente.

Chiamate di funzioni:

1) La chiamata alla funzione "**call SetWindowsHook()**" viene utilizzata per installare un hook di sistema, cioè un metodo dedicato al monitoraggio degli eventi di una data periferica, come ad esempio la tastiera o, come nel nostro caso, il mouse, e "**push WH_Mouse**" specifica che si sta installando un hook del mouse, ciò potrebbe, dunque, indicare un interesse nel monitorare e registrare l'input del mouse sul sistema.

"**push WH_Mouse**": Questa istruzione spinge il valore "WH_Mouse" sullo stack
"**call SetWindowsHook()**": Dopo aver caricato il tipo di hook sullo stack, viene effettuata la chiamata alla funzione "**SetWindowsHook()**". Questa funzione fa parte dell'API di Windows ed è utilizzata per installare hook del sistema

2) La sequenza di istruzioni **evidenziata in arancione** esegue un'operazione di copia file utilizzando la funzione di sistema "**CopyFile()**". La cartella di destinazione e il percorso del file da copiare sono passati come argomenti alla funzione.

"**push ecx**": Questa istruzione spinge il contenuto del registro ECX sullo stack. ECX è spesso utilizzato come registro di contatore in assembly, ma il commento successivo indica che ECX contiene il percorso della cartella di destinazione
"**push edx**": Questa istruzione spinge il contenuto del registro EDX sullo stack. EDX è un registro generale e, nel contesto del commento, contiene il percorso del file da copiare
"**call CopyFile()**": Questa istruzione chiama la funzione CopyFile(). Questa funzione fa parte dell'API di Windows ed è utilizzata per copiare un file da una posizione a un'altra. I parametri passati alla funzione sono i percorsi della cartella di destinazione e del file da copiare, che sono stati spinti sullo stack precedentemente

Quesito 2

Il metodo utilizzato dal malware per ottenere la persistenza sul sistema operativo è di tipo "**startup**", quindi il malware cerca di assicurare la sua esecuzione automatica copiandosi nella cartella di avvio del sistema, pertanto verrà eseguito ogni volta che il sistema si avvierà.
Questo lo possiamo rilevare dalle righe di codice **evidenziate in verde**, dove il percorso "startup_folder_system" sembra essere caricato da [EDI], e il percorso del malware è caricato da [ESI]. Il malware sembra quindi copiarsi in una posizione specifica nel sistema operativo, rendendolo eseguibile all'avvio del sistema (attraverso la parte evidenziata in arancione).