Esercizio 4 settimana 11

Analisi comportamentale delle categorie dei malware più note

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

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();	

- Identificazione del tipo di malware in base alle chiamate di funzione utilizzate.

Il malware utilizza la funzione SetWindowsHook per installazione di un hook per il controllo di un device. Vediamo anche come sia passato il parametro WH_Mouse sullo stack, per questo possiamo ipotizzare che il malware sia un kaylogger che registra la digitazione del mouse da parte dell'utente.

- Evidenzio le chiamate di funzione principali ed aggiungo una descrizione.

SetWindowsHook() Una funzione di hooking di Windows che permette di monitorare e intercettare gli eventi del sistema, come i messaggi di input della tastiera e del mouse. Nelle istruzioni fornite, viene chiamata con l'argomento WH_Mouse per registrare il malware come hook per la gestione degli eventi del mouse.

- CopyFile()

Una funzione di Windows utilizzata per copiare un file da un percorso di origine a uno di destinazione. Nel caso del malware in questione, sembra che la funzione venga utilizzata per copiare se stesso in una cartella del sistema di avvio al fine di ottenere la persistenza.

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

Il malware in questione cerca di ottenere la persistenza sul sistema operativo copiandosi in una cartella di avvio. Si può vedere che il malware utilizza la funzione di Windows CopyFile() per copiare se stesso in una cartella di sistema, che in questo caso sembra essere la cartella di avvio del sistema operativo. Il percorso di origine del file da copiare (path_to_Malware) è contenuto nella variabile ESI, invece il percorso di destinazione della copia (path to_startup_folder_system) è contenuto nella variabile EDI. In seguito, la funzione CopyFile() viene chiamata con questi due percorsi come argomenti per effettuare la copia. In questo modo, il malware cerca di garantirsi che venga eseguito all'avvio del sistema operativo e, quindi, di ottenere una persistenza sul sistema.

- Analisi di basso livello delle singole istruzioni.

00401010 push eax

Sposta il contenuto del registro eax sulla cima dello stack.

00401014 push ebx

Sposta il contenuto del registro ebx sulla cima dello stack.

0**0401018 push ecx**

Sposta il contenuto di una variabile chiamata ex sulla cima dello stack.

0040101C push WH_Mouse

Sposta il valore della costante WH_Mouse sulla cima dello stack. Questa costante viene utilizzata come argomento per la funzione SetWindowsHook().

0040101F call SetWindowsHook()

Chiama la funzione di Windows SetWindowsHook(), passando come argomento la costante WH_Mouse precedentemente spostata sulla cima dello stack.

00401040 XOR ECX,ECX

Effettua un'operazione di XOR bitwise tra il registro ECX e se stesso, impostandolo a zero.

00401044 mov ecx, [EDI]

Sposta il contenuto della variabile EDI nel registro

ECX. 00401048 mov edx, [ESI]

Sposta il contenuto della variabile ESI nel registro EDX.

0040104C push ecx

Sposta il contenuto del registro ECX sulla cima dello stack. Questo valore sarà utilizzato come percorso di destinazione per la funzione CopyFile().

0040104F push edx

Sposta il contenuto del registro EDX sulla cima dello stack. Questo valore sarà utilizzato come percorso di origine per la funzione CopyFile().

00401054 call CopyFile()

Chiama la funzione di Windows CopyFile(), passando come argomenti i due percorsi precedentemente spostati sulla cima dello stac