Funzionalità dei Malware

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();	

Traccia 1

Dalla chiamata di funzione SetWindowsHook() capiamo che si tratta di un keylogger poichè è una funzione comunemente usata da questi ultimi.

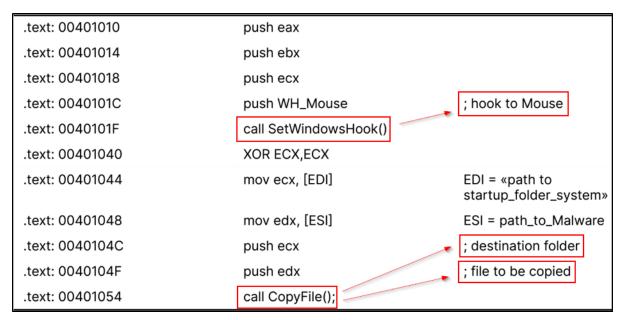


Traccia 2

Le chiamate di funzione principali sono le seguenti:

SetWindowsHook(): Questa funzione chiama SetWindowsHook per agganciare un hook, nel nostro caso al mouse.

CopyFile(): Questa funzione chiama CopyFile per copiare un file dalla cartella di destinazione (destination folder) al percorso specificato (file name).



Traccia 3

Il malware assicura la sua persistenza copiando il proprio eseguibile nella cartella di avvio del sistema operativo. Partendo dall'istruzione 00401040, viene inizializzato il registro ECX a 0, successivamente vengono impostati i percorsi della cartella di avvio del sistema e dell'eseguibile del malware nei registri ECX ed EDX. Quindi entrambi i registri vengono passati come argomenti alla funzione CopyFile() tramite le istruzioni push ECX e push EDX. La funzione CopyFile() eseguirà quindi la copia del contenuto di EDX (cioè l'eseguibile del malware) nella cartella di avvio del sistema operativo.

Traccia 4

push eax: Pusha il contenuto del registro EAX nello stack.

push ebx: Pusha il contenuto del registro EBX nello stack.

push ecx: Pusha il contenuto del registro ECX nello stack.

push WH_Mouse ;hook to Mouse: Pusha il valore della costante WH_Mouse nello stack.

call SetWindowsHook(): Chiama la funzione SetWindowsHook() con il parametro precedentemente pushato (WH_Mouse).

xor ecx,ecx: Esegue l'operazione XOR sul registro ECX, azzerandolo.

mov ecx, [edi]: Carica il valore puntato da EDI nel registro ECX.

mov edx, [esi]: Carica il valore puntato da ESI nel registro EDX.

push ecx: Pusha il contenuto del registro ECX nello stack.

push edx: Pusha il contenuto del registro EDX nello stack.

call CopyFile(): Chiama la funzione di sistema CopyFile() con i percorsi della cartella di avvio e dell'eseguibile del malware come parametri.