

S11/L4

Funzionalità dei Malware

Traccia:

La figura successiva mostra un estratto del codice di un malware.

Identificate:

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

.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();	

1.

Analizzando il malware possiamo notare la funzione **SetWindowsHook()** che serve per installare un metodo chiamato hook per monitorare una periferica, nel nostro caso il malware andrà ad “agganciarsi” al mouse tramite il push dell’hook **WH_Mouse**. Possiamo quindi affermare che si tratta di un **keylogger**.

.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	

Nel codice sono presenti due funzioni principali:

- **SetWindowsHook()**

Questa funzione installa un metodo (una funzione) chiamato “hook” dedicato al monitoraggio degli eventi di una data periferica come mouse o tastiera.

- **CopyFile()**

Questa funzione è progettata per copiare un file da una posizione a un'altra all'interno di un sistema operativo.

.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();	

2.

Per ottenere la persistenza il malware utilizza la tecnica dello “startup folder” che consiste nel copiarsi all’interno di una particolare cartella del sistema operativo che viene avviata all’avvio del sistema.

.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();	