Progetto S11L4

Alessandro Moscetti

Dovevamo rispondere ai seguenti quesiti riguardanti il codice proposto (in basso):

- 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 .

Codice proposto

.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();	

Punto 1

Possiamo intuire il tipo di malware (**keylogger**) dalla funzione SetWindowsHook(), questa funzione serve per installare un hook nel sistema.
Questa funzione ci permette di monitorare gli eventi di una determinata periferica in questo caso il mouse perchè vediamo che l'ultimo valore passato allo stack è WH_Mouse.

.text: 0040101C	push WH_Mouse	; hook to Mouse
.text: 0040101F	call SetWindowsHook()	

Punto 2

La persistenza del malware nel sistema avviene perché carica il suo file eseguibile nella cartella ‘startup_folder_system’ ossia la cartella di startup del sistema.
Questo avviene tramite la funzione CopyFile(), funzione che copia un file da una posizione a un’altra.

.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();	