Relazione S11L4

Nell'esercizio odierno è necessario definire:

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

Il codice da analizzare è il seguente:

.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();	

Analizzandolo è possibile vedere che il tipo di malware è un **keylogger,** si può determinare dal fatto che venga utilizzata la funzione **SetWindowsHook** e che nell'istruzione precedente venga pushato l'hook sul mouse. Quella funzione viene utilizzata appunto definendo un hook che monitora gli eventi del dispositivo target (in questo caso il mouse) e salverà le informazioni su un file di log.

.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();	

Per quanto riguarda la persistenza invece possiamo vedere che il malware la ottiene inserendosi nella **startup folder**, le istruzioni che ci mostrano ciò sono quelle mostrate sopra.

In pratica il malware si prende il path per la cartella di startup del sistema e ci copia il file malevolo chiamando la funzione **CopyFile()** e passandogli il path come parametro.

Davide Lecci