ANALISI MALWARE

L'esercizio di oggi ci richiede di analizzare il codice riportato qui sotto e di individuare il tipo di malware in base alle chiamate di funzione utilizzate e di individuare il metodo utilizzato per ottenere la persistenza

.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();	

Il tipo di malware è un keylogger che è programma per intercettare tutto ciò che l'utente della macchia infetta digita sulla tastiera.

Come possiamo notare dalla foto sotto infatti chiama la funzione SETWINDOWSHOOK che serve per monitorare gli eventi di una data periferica come ad esempio la tastiera o il mouse.

Il metodo HOOK verrà allertato ogni volta che l'utente digiterà un tasto sulla tastiera e salverà le informazioni su un file di Log

Nel nostro caso monitorerà gli eventi del mouse

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

Invece per la persistenza il malware usa il metodo startup_folder_system che è una particolare cartella del sistema operativo che viene controllata all'avvio del sistema .
Se un malware riesce a copiare il suo eseguibile all'interno delle cartelle di conseguenza verrà eseguito automaticamente all'avvio del sistema

.text: 00401044	mov ecx, [EDI]	EDI = «path to startup_folder_system»

Istruzione	Descrizione
Push eax	Parametri passati alla funzione
Push ebx	Parametri passati alla funzione
Push ecx	Parametri passati alla funzione
Push WH_mouse	Parametri passati alla funzione
Call setwindowshook	Chiamata della funzione
Xor ecx,ecx	Inizializza a 0 il registro ecx,infatti l'operatore logico tra due bit identici restituisce sempre 0
Mov ecx, [edi]	Copia il contenuto dell'indirizzo di memoria specificato da edi nel registro ecx
Mov edx, [esi]	Copia il contenuto dell'indirizzo di memoria specificato da esi nel registro edx
Push ecx	Parametri passati alla funzione
push edx	Parametri passati alla funzione
Call copy file	Chiamata della funzione