Analisi del comportamento di un Malware

Prendiamo in analisi il seguente codice Assembly

.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 & 2) Identificazione delle funzionalità principali del Malware
Per capire quale sia la funzionalità principale di questo virus dobbiamo basarci sulle conoscenze pregresse delle funzioni invocate nel codice Assembly.

push WH_Mouse: inizia la procedura di monitoraggio/ancoragio dei messaggi inviati dal mouse. Tale riga serve alla funzione successiva a indicare la periferica desiderata.
call SetWindowsHook(): Funzione utilizzata per monitorare e registrare tutti gli eventi di una data periferica tale procedura è detta HOOK ovvero ancoraggio. Inoltre questa funzione restituisce un file di log contenente tutti gli eventi che il malware è riuscito a registrare.

Possiamo rapidamente concludere il malware in analisi ha sicuramente la funzione di **KeyLogger** anche se in questo caso non viene monitorata la tastiera ma il mouse.

3)Analisi del metodo di persistenza
Per capire come il malware ottiene persistenza sul sistema operativo dato concentriamoci sulla seconda metà del codice Assembly.

mov ecx,[EDI]: Sposta il valore di EDI nel registro ecx. Come da nota vediamo che EDI contiene il path di una cartella di startup del sistema che il virus utilizza per avviarsi all'avvio del sistema operativo stesso. Probabilmente:
C:\Users\Guest\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

mov edx,[ESI]: Sposta il valore di ESI nel registro edx. Come da nota vediamo che ESI contiene il path del malware, questo servirà nella funzione successiva.

push ecx: salva nello stack il contenuto del registro ecx.

push edx: salva nello stack il contenuto del registro edx.

call CopyFile(): Chiama la funzione CopyFile. Funzione standard che copia il file del path contenuto nel registro edx nel path definito da ecx.

Analisi del comportamento di un Malware

4) Analisi di basso livello delle istruzioni.

push (eax,ebx,ecx): scrive sullo stack i valori di tali registri.

xor ecx,ecx: ripulisce il registro ecx