CONSEGNA SETTIMANA 11 LEZIONE 4

Funzionalità dei malware

Ci viene richiesto di analizzare il malware descritto e rispondere alle seguenti domande.

- **PUNTO 1. Identifica** il tipo di Malware in base alle chiamate di funzione utilizzate. Evidenziate le **chiamate di funzione** principali aggiungendo una descrizione per ognuna di essa
- **PUNTO 2.** Il metodo utilizzato dal Malware per ottenere la **persistenza** sul sistema operativo
- **BONUS:** Effettuare anche un'analisi basso livello delle singole istruzioni

.text: 00401010	push eax		Creazione dello stack
.text: 00401014	push ebx		
.text: 00401018	push ecx		
.text: 0040101C	push WH_Mouse	; hook to Mouse	Imposto il parametro e chiamo la funzione SetWindowsHook()
.text: 0040101F	call SetWindowsHook()		
.text: 00401040	XOR ECX,ECX		Eseguo uno XOR e imposto ECX a 0
.text: 00401044	mov ecx, [EDI]	EDI = «path to startup_folder_system»	Inserisco in ECX il path per la startup_folder_system
.text: 00401048	mov edx, [ESI]	ESI = path_to_Malware	Inserisco in EDX il path del Malware
.text: 0040104C	push ecx	; destination folder	Imposto i parametri e chiamo la funzione CopyFile()
.text: 0040104F	push edx	; file to be copied	
.text: 00401054	call CopyFile();		

PUNTO 1.

Il malware qui sopra rappresentato dal codice assembly pare sia in grado di auto propagarsi all'interno del sistema operativo senza l'input da parte di un utente. Date le istruzioni possiamo identificare il malware come un trojan oppure un worm, in quanto è in grado di diffondersi autonomamente nel sistema.

Le chiamate alle funzioni presenti nel frammento di codice sono 2:

- **Call SetWindowsHook()** – applica un hook che controlla l'input da parte del mouse (data l'istruzione *push WH_Mouse* precedente)
- **Call CopyFile()** – copia il file del malware all'interno del path indicato precedentemente (nel nostro caso la cartella *startup_folder_system*)

PUNTO 2.

Il Malware qui sopra descritto ottiene la persistenza nel sistema operativo copiandosi nella cartella di avvio del sistema (*startup_folder_system*). Nella cartella di avvio del sistema vengono posizionati i file eseguibili che devono essere avviati automaticamente all'avvio del sistema operativo. In questo modo il Malware otterrà la persistenza in quanto verrà eseguito automaticamente all'avvio del sistema operativo.