ES 4 U3W3

Traccia:

La figura nella slide successiva mostra un estratto del codice di un malware.
Identificate:

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

.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();	

Analisi del codice

1) il tipo di malware riguarda un KEYLOGGER ovvero un tipo di strumento di una periferica come tastiera o come in questo caso il mouse senza che l'utente se ne accorga.
2) Come vediamo sulla riga 5 nella funzione viene effettuata una call a SetWindowsHook che andrà ad interagire con il mouse e salverà le informazioni sui file di log,mentre nell'ultima riga vediamo il call copyfile,che nel momento in cui avrà identificato il dispositivo esterno copierà il file eseguibile in una cartella startup ottenendo l'avvio automatico
3) il metodo utilizzato per ottenere la persistenza è lo startup folder ovvero come detto in precedenza il malware copia il file eseguibile e lo rinomina come autorun

4) Analisi codice a basso livello:

PUSH EAX – inserisce il valore contenuto nel registro EAX in cima allo stack di memoria

PUSH EBX – inserisce il valore contenuto nel registro EBX in cima allo stack di memoria

PUSH ECX – inserisce il valore contenuto nel registro ECX in cima allo stack di memoria

PUSH WH_Mouse – Inserisce l'hook WH_Mouse per il monitoraggio del mouse in cima allo stack

Call SetWindowsHook() - Chiama la funzione SetWindowsHook() per configurare il monitoraggio della periferica esterna

XOR,ECX,ECX – Azzera il contenuto del registro ECX con l'operatore logico XOR

Mov,ECX,[EDI]- Copia il contenuto di [EDI] nel registro ECX

Mov,EDX,[ESI]- Copia il contenuto di [ESI] nel registro EDX

Push ECX- inserisce il valore del registro ECX in cima allo stack di memoria

Push EDX- inserisce il valore del registro EDX in cima allo stack di memoria

Call CopyFile() - Chiama la funzione CopyFile() per copiare un file