Funzionalità dei Malware

Traccia:

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

- Il tipo di Malware in base alle chiamate di funzione utilizzate. Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa
- Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo

.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. Il malware utilizza le istruzioni push per inserire i valori dei registri eax, ebx e ecx nello stack e l'istruzione call per chiamare la funzione SetWindowsHook.
   Tale funzione, in particolare, serve ad agganciare il mouse della vittima. Ciò ci suggerisce che si tratta di un **keylogger**, che, difatti, spesso utilizzano hook per monitorare l'input dell'utente.

2. Successivamente, il malware utilizza l'istruzione *XOR* per azzerare il registro ECX e le istruzioni *MOV* per spostare i valori dai registri EDI e ESI, rispettivamente nei registri ecx e edx. Questi valori vengono quindi inseriti nello stack utilizzando l'istruzione push e la funzione CopyFile. Quest'ultima funzione, in particolare, consente di monitorare determinati eventi del sistema, come l'input della tastiera o del mouse e di copiare un file da una posizione a un'altra.

In sintesi, l'estratto di codice mostra che il malware sta utilizzando la funzione **SetWindowsHook,** per agganciare il mouse e la funzione **CopyFile,** per copiare un file da una posizione specificata

in ESI a una destinazione specificata in EDI. Questo suggerisce che il malware sta cercando di ottenere persistenza sul sistema operativo copiandosi nella cartella di avvio del sistema