Amarfii Adrian 19/01/2023
Report
Task

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();	

In base alla funzione chiamata → call SetWindowsHook() si tratta di un keylogger ti categoria SetWindowsHook→ installa una funzione (hook) per monitorare per esempio la tastiere o il mouse

Come mantiene la persistenza ?Il metodo utilizzato da questo malware e il tipo Start up folder (una cartella che viene verificata e eseguita al avvio del sistema)come vediamo nel codice , il malware si copia nella cartella .Alla fine fa una chiamata alla funzione Copyfile per copiarsi li .

PUSH EAX/EBX/ECX → creazione dello stack
PUSH WH_MOUSE → push del hook nello stack
CALL SETWINDOWSHOOK→ chiamata a funzione che carichera il hook
XOR ECX ECX → registro ECX non inizializzato con valore 0
MOV ECX EDI → inserire in ECX il valore di EDI
MOV EDX ESI→ inserire in EDX il valore di ESI
PUSH ECX/EDX→ push dei registri nello stack
CALL COPYFILE → chiamata alla funzione che copiera il malware nella startupfolder.