

A decorative graphic on the left side of the slide, consisting of a network of white lines and small circles on a blue gradient background, resembling a circuit board or a neural network.

ES LEZIONE 4 SETTIMANA 11

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

Figura 1:

.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°

- In questo caso parliamo di un "keylogger", include tutti quei malware che per catturare la digitazione utente fanno leva sulla funzione «SetWindowsHookEX».

Figura 1:

.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();	

2°

- "call SetWindowsHook()" Questa funzione non fa altro che installare un metodo (una funzione) chiamato «hook» dedicato al monitoraggio degli eventi di una data periferica, come ad esempio la tastiera o il mouse. Il metodo «hook» verrà allertato ogni qualvolta l'utente digiterà un tasto sulla tastiera e salverà le informazioni su un file di log.
- "call CopyFile()" il malware copia il suo eseguibile all'interno della cartella "startup_foulder"

Figura 1:

.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();	

4° Il Malware utilizza la tecnica dello «startup folder». E' una particolare cartella del sistema operativo che viene controllata all'avvio del sistema, ed i programmi che sono al suo interno vengono eseguiti. Se un Malware riesce correttamente a copiare il suo eseguibile all'interno di questa cartella, verrà di conseguenza eseguito automaticamente all'avvio del sistema.