ANALISI COMPORTAMENTALE MALWARE

.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();	

Cominciamo innanzitutto ad analizzare i vari passaggi contenuti nel codice:

Hook è un meccanismo tramite il quale un'applicazione può intercettare eventi;

WH_Mouse è usata per monitorare l'input del mouse;

SetWindowsHook è una funzione usata per installare l'hook;

Startup folder è una cartella di Windows che contiene tutti quei programmi che vengono eseguiti all'avvio del computer;

CopyFile è una funzione che copia un file esistente in un nuovo file.

Da questi passaggi capiamo che il malware vuole copiare sé stesso all'interno della cartella startup in modo da ottenere la persistenza andandosi ad inserire nei programmi che il sistema lancia automaticamente all'avvio del computer; per capire di che tipo è l'eseguibile dannoso, dobbiamo analizzare la funzione SetWindowsHook, la quale viene chiamata per installare il meccanismo che consente al malware di monitorare l'input del mouse e, conseguentemente, creare dei file di log con le informazione captate; capiamo quindi che il malware è chiaramente un KEYLOGGER, cioè quei programmi dannosi creati per intercettare specifici input.

1. **Identificare il tipo di malware in base alle funzioni utilizzate**

   Come già detto precedentemente, il malware è un KEYLOGGER.

2. **Evidenziare e descrivere le funzioni**

SetWindowsHook funzione usata per installare l'hook che verrà usato per il monitoraggio di una determinata periferica;

CopyFile funzione usata per copiare un file esistente in un nuovo file.

3. Metodo utilizzato per ottenere persistenza

Per ottenere persistenza, il malware copia sé stesso all'interno della cartella startup, cartella dove si trovano tutti i programmi che vengono automaticamente eseguiti all'avvio del computer.

4. Descrizione di ogni riga di codice

Push eax spinge il contenuto del registro eax in cima allo stack;
Push ebx spinge il contenuto del registro ebx in cima allo stack;
Push ecx spinge il contenuto del registro ecx in cima allo stack;
Push WH_Mouse spinge l'hook WH_Mouse in cima allo stack;
Call SetWindowsHook() chiama la funzione SetWindowsHook;
XOR ECX, ECX inizializza a 0 il registro ECX;
Mov ecx, [EDI] sposta il valore del registro EDI all'interno di ecx;
Mov edx, [ESI] sposta il valore del registro ESI all'interno di edx;
Push ecx spinge il contenuto del registro ecx in cima allo stack;
Push edx spinge il contenuto del registro edx in cima allo stack;
Call CopyFile() chiama la funzione CopyFIle.