Analisi di codice un malware

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();	

Identificazione del tipo di Malware in base alle chiamate di funzione utilizzate:

.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();	

Il malware chiama le funzioni:

SetWindowsHook
La funzione SetWindowsHook viene chiamata per monitorare gli eventi del mouse, probabilmente per intercettare attività dell'utente. Questo può indicare che si tratta di un malware di tipo spyware.

CopyFile
La funzione CopyFile viene chiamata per copiare un file da una posizione all'altra.

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();
```

Analizzando più a fondo la funzione CopyFile vedamo che il malware sta cercando di copiare un file da una cartella specifica (path_to_Malware) a un'altra (path to startup_folder_system). Se il file copiato è il malware stesso, significa che il malware copia se stesso nella cartella di startup del sistema. In questo modo il malware sarebbe avviato quando il sistema si avvia, ottenendo così la persistenza.

Analisi a Basso Livello delle 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()
```

In questo blocco di istruzioni viene effettuato un push dei valori dei registri EAX, EBX, ECX e WH_Mouse nello stack, che sono i parametri per la successiva call alla funzione SetWindowsHook, che parametrizzata in questo modo serve a monitorare gli eventi del mouse.

```
.text: 00401040    XOR ECX,ECX
```

Viene poi eseguita un'operazione XOR tra il registro ECX e se stesso, azzerandolo.

.text: 00401044	mov ecx, [EDI]	EDI = «path to startup_folder_system»
.text: 00401048	mov edx, [ESI]	ESI = path_to_Malware

mov ecx, [EDI] carica il valore dalla memoria all'indirizzo contenuto nel registro EDI nel registro ECX (EDI potrebbe essere il puntatore a una stringa contenente il percorso della cartella startup di sistema).

mov edx, [ESI] carica il valore dalla memoria all'indirizzo contenuto nel registro ESI nel registro EDX (ESI potrebbe essere il puntatore a una stringa contenente il percorso della cartella contenente il malware).

.text: 0040104C	push ecx	; destination folder
.text: 0040104F	push edx	; file to be copied
.text: 00401054	call CopyFile();	

In questo blocco di istruzioni viene effettuato un push dei valori dei registri ECX, EDX nello stack, che sono i parametri per la successiva call alla funzione CopyFile.

Il parametro “destination folder” è valorizzato con il registro ECX, che contiene il percorso della cartella startup di sistema.

Il parametro “file to be copied” è valorizzato con il registro EDX, che contiene il percorso della cartella contenente il malware.

Con queste istruzioni il malware copia se stesso nella cartella di startup del sistema.