

CS0424 S11-L4
FUNZIONALITA' DEI MALWARE

Mattia Fossati

22/08/2024

Traccia

00401010	push eax	
00401014	push ebx	
00401018	push ecx	
0040101C	push WH_Mouse	; hook to Mouse
0040101F	call SetWindowsHook()	
00401040	XOR ECX,ECX	
00401044	mov ecx, [EDI]	EDI = «path to startup_folder_system»
00401048	mov edx, [ESI]	ESI = path_to_Malware
0040104C	push ecx	; destination folder
0040104F	push edx	; file to be copied
00401054	call CopyFile();	

La figura 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. Effettuare anche un'analisi basso livello delle singole istruzioni.

1. Tipo di Malware

Il malware utilizza **2** chiamate di funzione, **SetWindowsHook** e **CopyFile**. Considerando le funzioni chiamate e i parametri passati ad esse, si potrebbe trattare di un **trojan** che ottiene persistenza sul sistema operativo e probabilmente installa un **keylogger** che registra gli input del mouse mouse.

```
push WH_Mouse           ; hook to Mouse  
call SetWindowsHook() ←
```

```
mov ecx, [EDI]           EDI = «path to  
                           startup_folder_system»  
mov edx, [ESI]           ESI = path_to_Malware  
push ecx                 ; destination folder  
push edx                 ; file to be copied  
call CopyFile(); ←
```

2. Chiamate di funzione

SetWindowsHook

```
push WH_Mouse           ; hook to Mouse  
call SetWindowsHook() ←
```

Questa funzione viene utilizzata per installare una procedura di hook per intercettare/monitorare/modificare gli input prima che raggiungano la destinazione. In questo caso specifico installa un hook per intercettare i segnali del mouse, essendo specificato il parametro **”WH_Mouse”**

CopyFile

```
mov ecx, [EDI]           EDI = «path to  
                           startup_folder_system»  
mov edx, [ESI]           ESI = path_to_Malware  
push ecx                 ; destination folder  
push edx                 ; file to be copied  
call CopyFile() ←
```

Questa funzione serve a copiare un file da una posizione a un'altra, in questo caso il malware copia se stesso nella cartella **”startup_folder_system”**

3. Persistenza sul Sistema

Il malware ottiene la persistenza sfruttando la funzione "**CopyFile**" appena descritta, infatti la cartella "**startup_folder_system**" contiene i programmi che vengono eseguiti automaticamente all' avvio del sistema operativo. Copiando se stesso in questa cartella, il malware verrà eseguito ogni volta che il sistema operativo verrà avviato.

4. Analisi a basso livello

```
push eax  
push ebx  
push ecx
```

Con push vengono salvati i registri eax, ebx e ecx nello stack.

```
push WH_Mouse           ; hook to Mouse
```

Viene passato l' argomento **MH_Mouse** alla funzione successiva.

```
call SetWindowsHook()
```

Viene chiamata la funzione **SetWindowsHook**.

```
XOR ECX,ECX
```

Con l' operatore **XOR** viene azzerato il valore di **ecx**.

<code>mov ecx, [EDI]</code>	<code>EDI = «path to startup_folder_system»</code>
<code>mov edx, [ESI]</code>	<code>ESI = path_to_Malware</code>

Viene copiato il percorso della cartella **startup_folder_system** nel registro **ecx** e il percorso del **malware** nel registro **edx**

<code>push ecx</code>	<code>; destination folder</code>
<code>push edx</code>	<code>; file to be copied</code>

Vengono pushati nello stack i registri **ecx** e **edx** come primo e secondo argomento per la funzione successiva.

<code>call CopyFile();</code>

Viene chiamata la funzione **CopyFile** per copiare il file (secondo argomento) dentro alla cartella di destinazione (primo argomento).