

S11/L4

Stefano Di Prospero

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

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();	

Da un primo sguardo al malware, le funzioni che utilizza portano a pensare ad un tipo di malware Keylogger, e tiene sotto controllo le attività non della tastiera ma del mouse.

2.

```
.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]
.text: 00401048          mov edx, [ESI]
.text: 0040104C          push ecx
.text: 0040104F          push edx
.text: 00401054          call CopyFile();
```

EDI = «path_to_startup_folder_system»
ESI = path_to_Malware
; destination folder
; file to be copied

Dall'analisi del codice si possono notare quali sono le funzioni chiamate:

- **SetWindowsHook();** il malware installa un metodo Hook che si occupa di monitorare gli eventi di una periferica.
- **push WH_Mouse;** l'hook viene effettuato sulla periferica mouse.

3.

```
.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]  
  
.text: 00401048          mov edx, [ESI]  
.text: 0040104C          push ecx          ; destination folder  
.text: 0040104F          push edx          ; file to be copied  
.text: 00401054          call CopyFile();
```

Il metodo del malware per ottenere la persistenza è quello di copiare la sua esecuzione all'interno della cartella di avvio

4.

.text: 00401010

push eax **si effettua la push di eax nello stack**

.text: 00401014

push ebx **push ebx nello stack**

.text: 00401018

push ecx **push di ecx nello stack**

.text: 0040101C

push WH_Mouse ; hook to Mouse

Hook della periferica mouse così da monitorare le attività di quella periferica

.text: 0040101F

call SetWindowsHook()

Chiamata della funzione SetWindowsHook per sfruttare l'hook su mouse e vedere cosa fa

.text: 00401040

XOR ECX,ECX

Inizializzazione del valore di ecx tramite l'utilizzo dello XOR , che quando compara lo stesso parametro lo porta a 0

.text: 00401044

mov ecx, [EDI]

EDI= «path to startup_folder_system»

Qui il malware copia la path della cartella di avvio del sistema nel parametro ecx

.text: 00401048

mov edx, [ESI]

ESI = path_to_Malware

Qui copia la sua destinazione in edx

.text: 0040104C

push ecx

; destination folder

Push di ecx con il valore aggiornato

.text: 0040104F

push edx

; file to be copied

Push di edx con il valore aggiornato

.text: 00401054

call CopyFile();

Utilizza la chiamata alla funzione CopyFiles per copiare i file nella cartella di avvio