Funzionalità dei Malware

Richieste

Il compito di oggi ci richiede di analizzare il malware presente sulle slide ed in particolare:

1. Il tipo di malware in base alle chiamate di funzione. Evidenziare le stesse e descrivere la loro funzionalità.
2. Il metodo utilizzato dal malware per ottenere la 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();
```

1. Il tipo del Malware

Il Malware in questione è molto probabilmente un **keylogger** e questo lo possiamo affermare grazie alle chiamate di funzione che individuiamo all'interno del codice:

- **SetWindowsHook()**: questa funzione installa un metodo, chiamato **<<hook>>** dedicato al monitoraggio degli eventi di una delle periferiche del nostro PC, in questo caso si tratta del **Mouse**;
- **CopyFile()**: questa funzione fa sì che il malware copi il suo file eseguibile all'interno del dispositivo.

  Dopo l'avvio della periferica, per far si che il malware sia eseguito automaticamente o mediante doppio click, basta rinominare il file in "***Autorun***".

2. Metodo utilizzato per la persistenza

La persistenza consiste nella capacità di un Malware di indurre un sistema operativo ad avviare il malware stesso automaticamente al suo avvio. Ci sono due modi principali attraverso i quali i malware cercano di sfruttare queste funzionalità e sono: scheduled task o startup folder.

Nel nostro caso si tratta di un **startup folder**. Questa è una cartella particolare dell'OS che viene controllata all'avvio del sistema ed i programmi che si trovano al suo interno vengono eseguiti. Il malware si insedia in una delle due cartelle, sia quella dedicata agli utenti che quella generica del sistema operativo, presenti e si avvia ogni volta che viene avviato il sistema.

4. Analisi a basso livello

ISTRUZIONE	DESCRIZIONE
push eax, ebx, ecx, WH_Mouse	Spinge sullo stack eax, ebx, ecx e WH_Mouse
call SetWindowsHook()	Chiama la funzione SetWindowsHook
XOR ECX, ECX	Azzera il registro ECX
mov ecx,[EDI]	Copia EDI in ecx
mov edx, [ESI]	Copia ESI in edx
push ecx, edx	Spinge ecx e edx sullo stack
call CopyFile()	Chiama la funzione CopyFile