Consegna S11-L4

Funzionalità dei Malware

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

Traccia

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();	

Il tipo di Malware

Il codice sospetto evidenzia due comportamenti tipici di un keylogger: l'installazione di un hook per monitorare l'input del mouse, solitamente utilizzato per rubare informazioni sensibili, e la copia di se stesso in una cartella di avvio del sistema, garantendo così la persistenza nel sistema infetto. Questa combinazione suggerisce un malware progettato per spiare le attività dell'utente e per garantire il suo funzionamento costante nel sistema, potenzialmente con scopi dannosi come il furto di informazioni o il controllo remoto del computer.

```
.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();
```

Funzioni principali

Le due principali chiamate di funzione nel codice assemby sono:

SetWindowsHook(): Stabilisce un hook nel sistema per monitorare gli eventi del mouse. Tale comportamento è spesso associato a malware progettati per intercettare e registrare l'input dell'utente, come le password o le attività di navigazione, potenzialmente per scopi fraudolenti.

CopyFile(): Copia un file in una nuova posizione. Nel contesto di un malware, viene utilizzata per garantire la persistenza nel sistema, copiando il malware stesso in una cartella di avvio del sistema. Questo assicura che il malware continui ad essere attivo e operativo anche dopo il riavvio del sistema.

```
.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();
```

Metodo per la persistenza

Il malware ottiene la persistenza sul sistema operativo copiandosi in una cartella di avvio del sistema. Questo è evidenziato dalla chiamata di funzione CopyFile() nel codice assembly. Il malware prende il suo percorso attuale (path_to_Malware) e lo copia nella cartella di avvio del sistema (path to startup_folder_system). Questa azione garantisce che il malware venga eseguito ogni volta che il sistema operativo viene avviato, mantenendo così la sua presenza nel sistema anche dopo un riavvio. Il tipo di metodo è chiamato «Startup Folder».

```
.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();
```

Analisi singole istruzioni

Push: Salva il valore dei registri eax, ebx, ecx nello stack.

push WH_Mouse: Mette l'indirizzo WH_Mouse nello stack come parametro.

call SetWindowsHook(): Chiama la funzione per installare un hook per il mouse.

XOR ECX,ECX: Azzera il registro ecx.

mov ecx, [EDI]: Carica il percorso della cartella di avvio nel registro ecx.

mov edx, [ESI]: Carica il percorso del malware nel registro edx.

push ecx: Mette il percorso della cartella di avvio nello stack.

push edx: Mette il percorso del malware nello stack.

call CopyFile(): Chiama la funzione per copiare il malware nella cartella di avvio.

```
.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();
```

Fine della presentazione

Amedeo Natalizi