Compito S11/L4

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

.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. Tipo di malware

Questo malware è un **keylogger**: un particolare tipo di malware programmato per intercettare tutto ciò che l'utente della macchina infetta digita sulla tastiera. Lo si capisce da questa parte di codice:

.text: 0040101C push WH_Mouse; hook to Mouse

.text: 0040101F call SetWindowsHook()

Dove **hook** è dedicato al monitoraggio degli eventi di una data periferica, come ad esempio la tastiera o il mouse. Il metodo **hook** verrà allertato ogni qualvolta l'utente digita un tasto sulla tastiera e salverà le informazioni su un file di log. La figura seguente mostra il metodo **hook** installato per monitorare gli eventi della tastiera del PC. Dopodiché, il malware farà leva sulla funzione **SetWindowsHook()**.

2. Funzioni Principali

SetWindowsHook(): Questa chiamata di funzione è utilizzata per impostare un hook del mouse. Gli hooks sono meccanismi di monitoraggio degli eventi di sistema in Windows. Nel contesto del malware, potrebbe essere utilizzato per rilevare o intercettare attività legate al mouse.

CopyFile(): Questa chiamata di funzione è utilizzata per copiare un file da una posizione a un'altra. Nel contesto del malware, questa azione potrebbe essere correlata alla propagazione del malware, copiandosi in un'altra posizione del sistema.

3. Persistenza

Questo malware, per ottenere persistenza su un sistema operativo Windows, copia il suo eseguibile in una delle cartelle di avvio (che sia la cartella dedicata a un utente specifico oppure la cartella di avvio comune a tutti gli utenti). Questa tecnica è chiamata **Startup folder**.

La startup folder è una particolare cartella del sistema operativo che viene controllata all'avvio del sistema, e i programmi che si trovano al suo interno vengono eseguiti.

Si capisce che il malware utilizza questo tipo di tecnica da questa parte di codice:

```
.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();
```

Bonus

Ecco una tabella con le descrizioni del codice:

Codice Assembly	Descrizione
.text: 00401010 push eax	Mette il valore del registro EAX nello stack.
.text: 00401014 push ebx	Mette il valore del registro EBX nello stack.
.text: 00401018 push ecx	Mette il valore del registro ECX nello stack.
.text: 0040101C push WH_Mouse ; hook to Mouse	Mette il valore della costante WH_Mouse nello stack. Presumibilmente, questa costante rappresenta un tipo di hook per il mouse.
.text: 0040101F call SetWindowsHook()	Chiama la funzione SetWindowsHook(), probabilmente per installare un hook di Windows, come indicato dal valore nello stack.
.text: 00401040 XOR ECX,ECX	Esegue un'operazione XOR sul registro ECX, azzerandolo.
.text: 00401044 mov ecx, [EDI] EDI = «path to startup_folder_system»	Muove il valore all'indirizzo contenuto in EDI nel registro ECX.
.text: 00401048 mov edx, [ESI] ESI = path_to_Malware	Muove il valore all'indirizzo contenuto in ESI nel registro EDX.
.text: 0040104C push ecx ; destination folder	Mette il valore di ECX nello stack (presumibilmente il percorso della cartella di avvio del sistema).
.text: 0040104F push edx ; file to be copied	Mette il valore di EDX nello stack (presumibilmente il percorso del malware).
.text: 00401054 call CopyFile()	Chiama la funzione CopyFile() per copiare un file dal percorso del malware al percorso della cartella di avvio del sistema.