Report di analisi e soluzione del codice malware

Introduzione

In questa esercitazione, ho analizzato un estratto di codice malware per identificare il tipo di malware, il metodo utilizzato per ottenere la persistenza sul sistema operativo e ho effettuato un'analisi a basso livello delle singole istruzioni. Di seguito riporto in dettaglio l'intero processo di analisi e la soluzione finale.

Identificazione del Tipo di Malware

La figura riportata (Figura 1) mostra un estratto del codice del malware. La prima parte del codice utilizza la funzione SetWindowsHook, una funzione tipicamente usata per installare un hook nella catena di hook di Windows, permettendo di monitorare gli eventi del sistema. Questo particolare codice utilizza il parametro WH_MOUSE, indicando che l'hook è relativo agli eventi del mouse. La presenza di questa chiamata suggerisce che il malware è un **keylogger** o **spyware**, che tenta di raccogliere informazioni sulle azioni dell'utente monitorando il mouse.

Chiamate di Funzione e Descrizione

1. **SetWindowsHook()**
    - **Descrizione:** Questa funzione è utilizzata per installare un hook di sistema. Nel nostro caso, il parametro WH_MOUSE indica che il malware sta monitorando gli eventi del mouse.
    - **Tipo di Malware:** L'uso di questa funzione è tipico dei keylogger o spyware che cercano di intercettare le azioni dell'utente.
2. **CopyFile()**
    - **Descrizione:** La funzione CopyFile è usata per copiare un file da un percorso sorgente a un percorso di destinazione. In questo caso, il malware utilizza questa funzione per copiare se stesso in una cartella di avvio del sistema operativo.
    - **Tipo di Malware:** Questo comportamento è tipico dei trojan o virus che cercano di ottenere persistenza copiando se stessi in una posizione da cui verranno eseguiti automaticamente.

Metodo di Persistenza

Il malware utilizza un metodo chiaro e diretto per ottenere persistenza copiando il proprio eseguibile nella cartella di avvio del sistema operativo. Questo processo è evidenziato nelle istruzioni che coinvolgono i registri EDI e ESI e la funzione CopyFile().

Dettagli delle Istruzioni di Persistenza

1. **mov ecx, [EDI]**: Carica il percorso della cartella di avvio del sistema operativo nel registro ECX. Questo percorso è dove il malware intende copiare se stesso per garantire l'esecuzione all'avvio.
2. **mov edx, [ESI]**: Carica il percorso del file del malware nel registro EDX.
3. **push ecx**: Inserisce il percorso di destinazione (cartella di avvio) nello stack.
4. **push edx**: Inserisce il percorso sorgente (file del malware) nello stack.
5. **call CopyFile()**: Chiama la funzione CopyFile per copiare il malware nella cartella di avvio, garantendo che venga eseguito ogni volta che il sistema si avvia.

Analisi a Basso Livello delle Singole Istruzioni

Di seguito riporto l'analisi dettagliata di ogni istruzione nel codice, per comprendere meglio le operazioni eseguite dal malware:

1. **push eax**: Salva il valore di eax sullo stack per preservare il suo stato attuale.
2. **push ebx**: Salva il valore di ebx sullo stack.
3. **push ecx**: Salva il valore di ecx sullo stack.
4. **push WH_Mouse**: Spinge il valore WH_MOUSE sullo stack. Questo valore è una costante che rappresenta un hook del mouse.
5. **call SetWindowsHook()**: Chiama la funzione SetWindowsHook per impostare un hook che monitora gli eventi del mouse.
6. **XOR ECX, ECX**: Azzeramento del registro ECX usando l'operazione XOR.
7. **mov ecx, [EDI]**: Carica il percorso della cartella di avvio del sistema nel registro ECX.
8. **mov edx, [ESI]**: Carica il percorso del file del malware nel registro EDX.
9. **push ecx**: Inserisce il percorso di destinazione nello stack.
10. **push edx**: Inserisce il percorso sorgente nello stack.
11. **call CopyFile()**: Chiama la funzione CopyFile per copiare il file del malware nella cartella di avvio.

Conclusione

L'analisi dettagliata del codice malware ha rivelato che si tratta probabilmente di un keylogger o spyware, con funzionalità per monitorare gli eventi del mouse. Inoltre, il malware utilizza un metodo di persistenza tipico dei trojan o virus, copiando se stesso nella cartella di avvio del sistema operativo. Questa esercitazione mi ha permesso di comprendere meglio le tecniche utilizzate dai malware per monitorare le attività degli utenti e garantire la loro persistenza su un sistema infettato.