Report di Analisi del Malware "Malware_U3_W3_L2"

Introduzione

L'obiettivo di questa esercitazione è acquisire esperienza nell'utilizzo di IDA Pro, uno strumento fondamentale per l'analisi statica del malware. In particolare, analizzerò un campione di malware chiamato "Malware_U3_W3_L2" per rispondere a una serie di quesiti specifici. Durante l'analisi, individuerò l'indirizzo della funzione DLLMain, l'indirizzo dell'import della funzione gethostbyname, il numero di variabili locali di una specifica funzione e il numero di parametri della stessa funzione. Infine, fornirò alcune considerazioni generali sul malware.

Configurazione di IDA Pro

Prima di iniziare con l'analisi, è necessario configurare correttamente IDA Pro.

1. **Installazione di IDA Pro**:
    - Scarica IDA Pro dal sito ufficiale Hex-Rays.
    - Segui le istruzioni per l'installazione sul tuo sistema operativo.
2. **Caricamento del binario**:
    - Avvia IDA Pro.
    - Seleziona File -> Open e carica il file binario del malware "Malware_U3_W3_L2".
    - Se IDA Pro chiede il tipo di file, seleziona il formato corretto (es. PE per eseguibili Windows).
3. **Configurazione dell'interfaccia**:
    - Assicurati che le seguenti finestre siano visibili: Funzioni, Imports, Exports, e Disassembly.
    - Puoi configurare queste finestre dal menu View.

1. Individuare l'indirizzo della funzione DLLMain

Per trovare l'indirizzo della funzione DLLMain, ho seguito i seguenti passaggi:

1. **Identificazione della funzione DLLMain**:
    - Dopo aver caricato il binario in IDA Pro, ho cercato la funzione DLLMain nella lista delle funzioni. Questa lista è disponibile nel pannello di sinistra sotto "Functions".
    - Ho trovato la funzione DLLMain e annotato il suo indirizzo.
2. **Annotazione dell'indirizzo**:
    - L'indirizzo della funzione DLLMain è 1000D02E, come mostrato nell'immagine seguente.

2. Individuare la funzione gethostbyname nella scheda «imports»

Per individuare l'indirizzo della funzione gethostbyname, ho eseguito i seguenti passaggi:

1. **Apertura della scheda Imports**:
    - Ho aperto la scheda Imports in IDA Pro, che elenca tutte le funzioni importate da altre librerie.
    - Questa scheda si trova solitamente nel pannello di sinistra.
2. **Ricerca della funzione gethostbyname**:
    - Ho scansionato la lista delle funzioni importate fino a trovare gethostbyname.
    - Ho annotato l'indirizzo dell'import, che è 100163CC.

3. Contare le variabili locali della funzione alla locazione di memoria 0x10001656

Per determinare il numero di variabili locali della funzione situata alla locazione di memoria 0x10001656, ho seguito questi passaggi:

1. **Navigazione alla locazione di memoria**:
    - Ho usato la barra degli indirizzi di IDA Pro per navigare direttamente alla locazione di memoria 0x10001656.
2. **Identificazione della funzione**:
    - Ho determinato a quale funzione appartiene questa locazione. La locazione appartiene alla funzione sub_10001656.
3. **Conteggio delle variabili locali**:
    - Esaminando lo stack frame della funzione identificata, ho trovato un totale di 20 variabili locali, tutte dichiarate con offset negativo rispetto al registro EBP.

4. Contare i parametri della funzione

Nella stessa funzione sub_10001656, ho analizzato i parametri passati. Ho seguito questi passaggi:

1. **Esame dei parametri della funzione**:
    - Ho analizzato l'inizio della funzione sub_10001656 dove vengono gestiti i parametri.
    - Ho identificato un solo parametro, denominato arg_0.

Considerazioni Finali

Dall'analisi effettuata, ho potuto dedurre diverse caratteristiche del malware "Malware_U3_W3_L2":

- **Interazione di Rete**: La presenza della funzione gethostbyname indica che il malware potrebbe comunicare con server remoti, suggerendo che potrebbe essere coinvolto in attività di esfiltrazione di dati o comando e controllo (C2).
- **Persistenza**: Non sono stati trovati indizi diretti su tecniche di persistenza, ma ulteriori analisi potrebbero rivelare modifiche a chiavi di registro o file di sistema che assicurano la persistenza del malware.
- **Offuscamento**: Non sono stati identificati metodi di offuscamento evidenti, ma la complessità del codice potrebbe indicare l'uso di tecniche per confondere l'analisi.
- **Payload**: Il malware sembra essere progettato per interagire con la rete e potenzialmente esfiltrare dati o ricevere comandi remoti. Ulteriori analisi delle funzioni di rete potrebbero confermare questa ipotesi.

Conclusione

L'analisi del malware "Malware_U3_W3_L2" ha fornito importanti informazioni sul suo funzionamento e sulle potenziali minacce che rappresenta. L'utilizzo di IDA Pro si è rivelato essenziale per individuare le funzioni critiche e comprendere la struttura interna del malware. Continuerò ad approfondire l'analisi per identificare ulteriori dettagli e migliorare le difese contro questo tipo di minacce.