Analisi statica avanzata con IDA

Traccia:

Lo scopo dell’esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l’analisi statica. A tal proposito, con riferimento al malware chiamato «Malware\_U3\_W3\_L2» presente all’interno della cartella «Esercizio\_Pratico\_U3\_W3\_L2» sul Desktop della macchina virtuale dedicata all’analisi dei malware, rispondere ai seguenti quesiti, utilizzando IDA Pro.

1. Individuare l’indirizzo della funzione DLLMain(così com’è, in esadecimale)

2. Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l’indirizzo dell’import? Cosa fa la funzione?

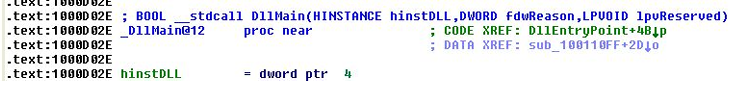
3. Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656?

4. Quanti sono, invece, i parametri della funzione sopra?

5. Inserire altre considerazioni macro-livello sul malware (comportamento)

Soluzione:

1) Per localizzare l'indirizzo della funzione DLLMain, dobbiamo aprire l'eseguibile con IDA Pro. Successivamente, cambiamo alla visualizzazione testuale usando la barra spaziatrice e cerchiamo l'indirizzo della funzione principale, che in questo caso è: 1000D02E.



Top of Form

2) Per determinare l'indirizzo dell'importazione di "gethostbyname", apriamo il pannello degli import in IDA Pro per trovare la funzione di interesse.

L'indirizzo associato a "gethostbyname" è 100163CC, come si può vedere nell'immagine.

La funzione **gethostbyname** è una funzione di rete utilizzata nelle applicazioni che utilizzano il protocollo TCP/IP. È parte delle librerie di socket Berkeley (BSD) e viene usata per recuperare le informazioni dell'host, come l'indirizzo IP, a partire dal nome dell'host.

A screenshot of a computer

Description automatically generated

3) Alla locazione di memoria 0x10001656 troviamo 20 variabili

A computer screen shot of a computer code

Description automatically generated

4) è presente un unico parametro in ingresso per la funzione, il quale possiede un offset positivo in relazione al registro EBP. Nell'analisi effettuata da IDA, questo parametro è etichettato come "arg\_0".

A computer screen shot of a code

Description automatically generated

5) Questo malware sembrerebbe voler collezzionare informazioni sull’host come l’indirizzo ip in cui è presente e comunicarle esternamente.