ESERCITAZIONE WEEK 23 DAY 5

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?
3. Quante sono le variabili locali della **funzione** alla locazione di memoria 0×10001656?
4. Quanti sono, invece, i parametri della funzione sopra?
5. Inserire altre considerazioni macro livello sul malware

---

1. L'indirizzo della funzione DLLMain è: 1000D02E;
2. L'indirizzo della funzione gethostbyname è 100163CC;
3. Le variabili locali della funzione all'indirizzo di memoria 0x10001656 sono 23;
4. C'è solo un parametro;
5. Analisi della barra di navigazione del codice:

È interessante notare che mentre il DLLMain che è una funzione scritta dal codice del malware, si trova nella sezione blu della barra, la funzione importata gethostbyname si trova nella sezone fucsia .idata ad indicare che è un'importazione esterna. Infatti questa sezione contiene le tabelle di importazione, che elencano i nomi delle funzioni o dei simboli che il programma deve trovare ed eseguire durante l'esecuzione.