CS0204

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.

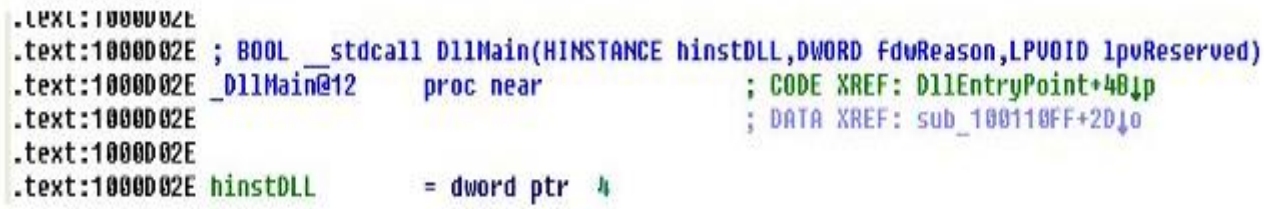
1. Individuare l'indirizzodella funzione DLLMain(così com'è, in esadecimale)

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

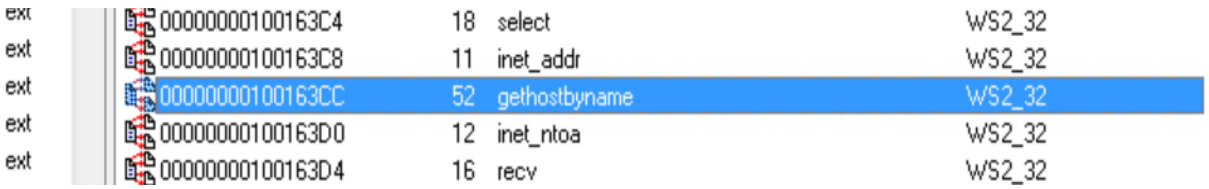
3. Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656?

4. Quanti sono, invece, i parametri della funzione sopra? 5. Inserire altre considerazioni macro livello sul malware (comportamento)

1. Carichiamo l'eseguibile in IDA Pro, una volta fatto, premiamo la barra spaziatrice per passare nella modalità testuale e recuperare l'indirizzo della funzione DllMain che sarà: 1000D02E.



2. Apriamo la finestra degli «imports» da IDA Pro, e localizziamo la funzione cercata. «gesthostbyname» è all'indirizzo **100163CC**, come mostrato in figura.



La funzione gesthostbyname recupera le informazioni host corrispondenti a un nome host da un database host.

3. Per prima cosa bisogna spostarsi all'indirizzo ricercato tramite la ricerca o la barra laterale. A questo indirizzo troviamo 20 variabili con offset negativo rispetto ad EBP

```
.text:10001656
.text:10001656 var_675         = byte ptr -675h
.text:10001656 var_674         = dword ptr -674h
.text:10001656 hLibModule      = dword ptr -670h
.text:10001656 timeout         = timeval ptr -66Ch
.text:10001656 name            = sockaddr ptr -664h
.text:10001656 var_654         = word ptr -654h
.text:10001656 Dst             = dword ptr -650h
.text:10001656 Parameter       = byte ptr -644h
.text:10001656 var_640         = byte ptr -640h
.text:10001656 CommandLine     = byte ptr -63Fh
.text:10001656 Source          = byte ptr -63Dh
.text:10001656 Data            = byte ptr -638h
.text:10001656 var_637         = byte ptr -637h
.text:10001656 var_544         = dword ptr -544h
.text:10001656 var_50C         = dword ptr -50Ch
.text:10001656 var_500         = dword ptr -500h
.text:10001656 Buf2            = byte ptr -4FCh
.text:10001656 readfds         = fd_set ptr -4BCh
.text:10001656 phkResult       = byte ptr -3B8h
.text:10001656 var_3B0         = dword ptr -3B0h
.text:10001656 var_1A4         = dword ptr -1A4h
.text:10001656 var_194         = dword ptr -194h
.text:10001656 WSAData         = WSAData ptr -190h
.text:10001656 arg_0           = dword ptr  4
```

4. Dalla stessa figura, possiamo notare un solo argomento passato alla funzione, avente offset positivo rispetto ad EBP. IDA ha chiamato questo parametro «arg_0».