## Esercitazione WEEK 23 D4 Analisi statica avanzata con IDA

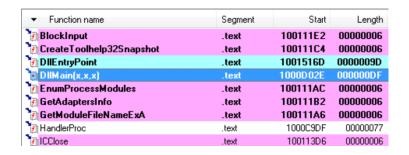
**Ettore Farris** 

## **Descrizione sintetica**

Traccia:

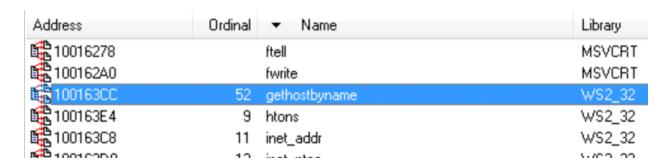
Lo scopo dell'esercizio è di acquisire esperienza con IDA, un tool fondamentale per l'analisi statica. A tal proposito, con riferimento al malware chiamato 
«Malware\_U3\_W3\_L2» presente all'interno della cartella 
«Esercizio\_Pratico\_U3\_W3\_L2» sul Desktop della macchina virtuale dedicata all'analisi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

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



La funzione DLLMain si trova all'indirizzo 1000D02E. L'informazione la si ottiene dalla Functions Window.

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



Dalla scheda imports vediamo che la funzione è all'indirizzo 100163CC.

- 3. Quante sono le variabili locali della **funzione** alla locazione di memoria 0x10001656?
- 4. Quanti sono, invece, i parametri della funzione sopra?

```
.text:18001656 ; ------ S U B R O U T I N E -----
.text:10001656
.text:10001656
.text:10001656 ; DWDRD __stdcall sub_10001656(LPV0ID)
.text:10001656 sub_10001656 proc near
                                                           ; DATA XREF: DllMain(x,x,x)+C8to
.text:10001656
= byte ptr -675h
.text:10001656 var 674
                                 = dword ptr -674h
.text:10001656 hLibModule
                                = dword ptr -670h
                                = timeval ptr -66Ch
= sockaddr ptr -664h
= word ptr -654h
= dword ptr -658h
.text:10001656 timeout
.text:10001656 name
.text:10001656 var_654
.text:10001656 Dst
                                = byte ptr -644h
= byte ptr -640h
.text:10001656 Parameter
.text:10001656 var_640
.text:10001656 CommandLine
                                 = byte ptr -63Fh
.text:10001656 Source
                                 = byte ptr -63Dh
.text:10001656 Data
                                 = byte ptr -638h
.text:10001656 var_637
.text:10001656 var_544
.text:10001656 var_500
                                = byte ptr -637h
= dword ptr -544h
= dword ptr -50Ch
                                 = dword ptr -500h
= byte ptr -4FCh
.text:10001656 var_500
.text:10001656 Buf2
.text:10001656 readfds
                                 = fd_set ptr -4BCh
                                = byte ptr -3B8h
.text:10001656 phkResult
.text:10001656 var_380
                                = dword ptr -3B0h
.text:10001656 var_1A4
                                 = dword ptr -1A4h
                                 = dword ptr -194h
.text:10001656 var_194
.text:10001656 WSAData
                                 = WSAData ptr -190h
.text:10001656 arg_0
                                 = dword ptr 4
```

La funzione ha 23 variabili e 1 parametro chiamato  $arg\_0$ . Questo lo si capisce dal segno dell'offset (negativo per le variabili e positivo per i parametri).

- 5. Inserire altre considerazioni macro livello sul malware

L'eseguibile è un trojan con una backdoor. Consultando le funzioni a cui accede, il malware ha accesso al file system e può manipolare i file, può manipolare il registro di sistema e può effettuare connessioni di rete. Inoltre intercetta i movimenti del mouse.