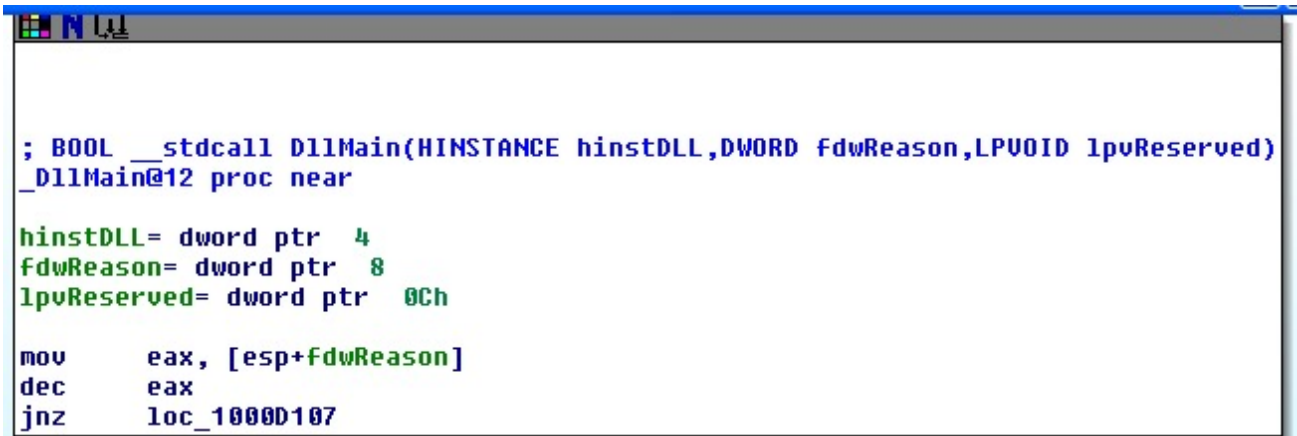


Analisi Statica Avanzata con IDA

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 0x10001656?
 4. Quanti sono, invece, i parametri della funzione sopra?
 5. Inserire altre considerazioni macro livello sul malware (comportamento)
-
1. Apro l'eseguibile con IDA e all'inizio del codice trovo immediatamente la funzione DllMain. Se non l'avessi trovata subito avrei usato la barra spaziatrice per passare alla modalità testuale e avrei cercato "DllMain"

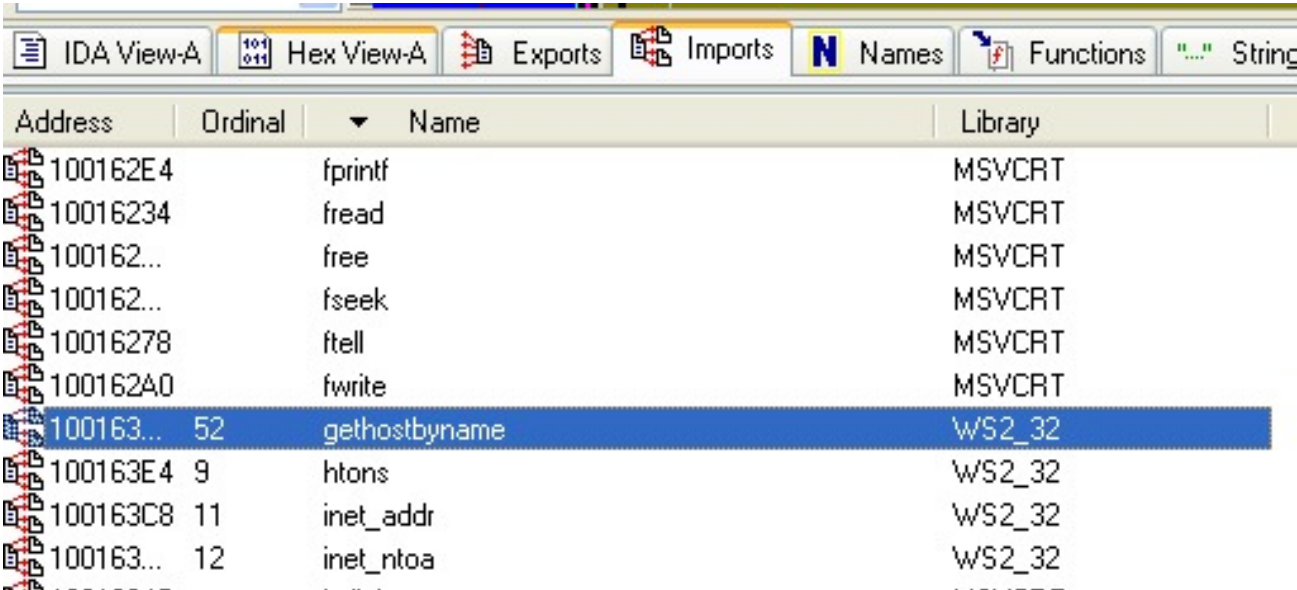


```
; BOOL __stdcall DllMain(HINSTANCE hinstDLL,DWORD fdwReason,LPUVOID lpvReserved)
_DllMain@12 proc near

hinstDLL= dword ptr 4
fdwReason= dword ptr 8
lpvReserved= dword ptr 0Ch

mov     eax, [esp+fdwReason]
dec     eax
jnz     loc_1000D107
```

2. Vado sulla scheda Imports e ordino i risultati per nome, trovo facilmente la funzione "gethostbyname"



Address	Ordinal	Name	Library
100162E4		fprintf	MSVCRT
10016234		fread	MSVCRT
100162...		free	MSVCRT
100162...		fseek	MSVCRT
10016278		ftell	MSVCRT
100162A0		fwrite	MSVCRT
100163...	52	gethostbyname	WS2_32
100163E4	9	htons	WS2_32
100163C8	11	inet_addr	WS2_32
100163...	12	inet_ntoa	WS2_32

3. Le funzioni che corrisponde all'indirizzo di memoria 10001656, contiene molte variabili locali: hanno tutte un offset negativo e sono 20. (Nello screen di seguito mancano le ultime 2)

```

; DWORD __stdcall sub_10001656(LPVOID)
sub_10001656 proc near

var_675= byte ptr -675h
var_674= dword ptr -674h
hModule= dword ptr -670h
timeout= timeval ptr -66Ch
name= sockaddr ptr -664h
var_654= word ptr -654h
in= in_addr ptr -650h
Parameter= byte ptr -644h
CommandLine= byte ptr -63Fh
Data= byte ptr -638h
var_544= dword ptr -544h
var_50C= dword ptr -50Ch
var_500= dword ptr -500h
var_4FC= dword ptr -4FC
readfds= fd_set ptr -4BCh
phkResult= HKEY__ ptr -3B8h
var_3B0= dword ptr -3B0h
var_1A4= dword ptr -1A4h

10001656: sub_10001656
Down Disk: 54GB

```

4. Il parametro della funzione sopra è il seguente

arg_0= dword ptr 4

5. Argomentazioni sul comportamento del malware

Il malware è probabilmente una backdoor che da informazioni sul sistema operativo e sulle configurazioni dello stesso. Se riconosce che è una macchina virtuale blocca il flusso informativo. "Display dns" ti fa vedere la cache dns. "Flash dns" mostra la cache locale