1. Individuare l’indirizzo della funzione DLLMain

Come possiamo vedere, l'indirizzo è 1000D02E, infatti vediamo la funzione dichiarata con i suoi parametri.

```
_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. Dalla scheda «imports» individuare la funzione «gethostbyname».


Individuata la funzione possiamo vedere che l'indirizzo dell'import è 100163CC e se utilizziamo il jump dando in input l'indirizzo di memoria vediamo che la funzione viene chiamata.

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

```
.text:10001656 ; DWORD __stdcall sub_10001656(LPVOID)
.text:10001656 sub_10001656    proc near               ; DATA XREF: DllMain(x,x,x)+C8↓o
.text:10001656
.text:10001656 var_675         = byte ptr -675h
.text:10001656 var_674         = dword ptr -674h
.text:10001656 hModule         = dword ptr -670h
.text:10001656 timeout         = timeval ptr -66Ch
.text:10001656 name            = sockaddr ptr -664h
.text:10001656 var_654         = word ptr -654h
.text:10001656 in              = in_addr ptr -650h
.text:10001656 Parameter       = byte ptr -644h
.text:10001656 CommandLine     = byte ptr -63Fh
.text:10001656 Data            = byte ptr -638h
.text:10001656 var_544         = dword ptr -544h
.text:10001656 var_50C         = dword ptr -50Ch
.text:10001656 var_500         = dword ptr -500h
.text:10001656 var_4FC         = dword ptr -4FCh
.text:10001656 readfds         = fd_set ptr -4BCh
.text:10001656 phkResult       = HKEY__ 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
```

Nella subroutine sono presenti varie variabili, precisamente 20. Come discusso in precedenza durante le lezioni, quando l'offset è negativo si fa riferimento alle variabili, mentre se è positivo si tratta di parametri. Pertanto, poiché l'offset dell'ultimo valore è positivo, questo sarà considerato un parametro.

4. Quanti sono, i parametri della funzione sopra?

L'unico parametro è l'ultimo arg 0.

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

Dalle mie osservazioni, sembra che il malware sia una backdoor. Questo può essere dedotto dal fatto che contiene sia le funzioni di invio (send) che di ricezione (recv). Inoltre, si nota che il malware stabilisce una connessione all'avvio, il che suggerisce che tenga traccia dei dati e delle azioni dell'utente.