



ANALISI STATICA AVANZATA CON IDA

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

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

```
1000D02E 8B 44 24 08 48 0F 85 CE 00 00 00 8B 44 24 04 53 ID$.H.à+...ID$.S
```

L'indirizzo usato dalla funzione è 1000D02E.

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

```
100163CC 52 gethostbyname WS2_32
```

gethostbyname è utilizzata per individuare l'indirizzo IP di un host.

```
struct hostent *__stdcall gethostbyname(const char *name)  
extrn gethostbyname:dword
```

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

Le variabili locali sono 23

```
sub_10001656 proc near
var_675= byte ptr -675h
var_674= dword ptr -674h
hLibModule= dword ptr -670h
timeout= timeval ptr -66Ch
name= sockaddr ptr -664h
var_654= word ptr -654h
Dst= duord ptr -650h
Parameter= byte ptr -644h
var_640= byte ptr -640h
CommandLine= byte ptr -63Fh
Source= byte ptr -63Dh
Data= byte ptr -638h
var_637= byte ptr -637h
var_544= dword ptr -544h
var_50C= dword ptr -50Ch
var_500= dword ptr -500h
Buf2= byte ptr -4FCh
readfds= fd_set ptr -48Ch
phkResult= byte ptr -388h
var_380= dword ptr -380h
var_1A4= dword ptr -1A4h
var_194= dword ptr -194h
WSAData= WSAData ptr -190h
arg_0= dword ptr 4
```

4. Quanti sono, invece, i **parametri** della funzione sopra?

I parametri sono solo 1:

```
arg_0= dword ptr 4
```

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

Deduco sia una backdoor poiché troviamo funzioni e variabili inerenti ad un'ipotetica "backdoorserver"

```
push    eax                ; lpBuffer
push    edi                ; nBufferLength
call    ds:GetCurrentDirectoryA
mov     esi, ds:sprintf
lea     eax, [ebp+buf]
push    offset aBackdoorServer ; "\\r\n\r\n*****\\r\n[Ba"...
push    eax                ; Dest
call    esi ; sprintf
mov     ebx, [ebp+5]
lea     eax, [ebp+buf]
push    eax                ; buf
push    ebx                ; s
call    sub_1000388B
add     esp, 10h
lea     eax, [ebp+PathName]
push    eax                ; lpPathName
call    ds:SetCurrentDirectoryA
test    eax, eax
jz      loc_100046E1
```