

# FUNZIONE DLLMAIN

Apriamo il file con Ida e tramite la barra di ricerca cerchiamo la funzione DLLMAIN

```
; 0001 __stdcall DllMain(HINSTANCE hinstDLL,DWORD fdwReason,LPOVOID lpvReserved)
_DllMain@12 proc near

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

# FUNZIONE GETHOSTBYNAME

La funzione gethostbyname recupera informazioni host corrispondenti a un nome host da un database host

Address	Ordinal	Name	Library
100162A0		fwrite	MSVCRT
100163...	52	gethostbyname	WS2_32
100163F4	9	htonl	WS2_32

# VARIABILI LOCALI DELLA FUNZIONE ALLA LOCAZIONE DI MEMORIA 0X10001656

```
.text:10001656
.text:10001656 ; DWORD __stdcall sub_10001656(LPOVOID)
.text:10001656 sub_10001656 proc near ; DATA XREF: DllMain(x,x,x)+C81d
.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 -48Ch
.text:10001656 phkResult = HKEY__ ptr -388h
.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 -48Ch
.text:10001656 phkResult = HKEY__ ptr -388h
.text:10001656 var_380 = dword ptr -380h
.text:10001656 var_1A4 = dword ptr -1A4h
.text:10001656 var_194 = dword ptr -194h
.text:10001656 WSADATA = WSADATA ptr -190h
```

