

# Malware Analysis con IDA

# Compito di oggi:

Lo scopo dell'esercizio di oggi è quello di andare ad analizzare il file infetto "Malware\_U3\_W3\_L2" con il tool IDA Pro. Le richieste sono le seguenti:

1. Individuare l'indirizzo della funzione DLLMain
2. Individuare la funzione gethostbyname
3. Quante sono le variabili locali alla locazione di memoria 0x10001656
4. Quanti sono i parametri della funzione

IDA Pro è un **disassembler** utilizzato per i file eseguibili, noi ci concentreremo sul formato PE.

# 1. Indirizzo funzione DLLMain



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

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

La prima parte del codice che appare, come mostra la foto qui sopra, è stata riconosciuta da IDA Pro durante la traduzione e rappresenta una parte della funzione `'main'`.

L'indirizzo trovato nel "name window" è 1000D02E

## 2. Funzione gethostbyname

100162A0		fwrite	MSVCRT
100163CC	52	gethostbyname	WS2_32
100163E4	9	htons	WS2_32
100163F0	11	inet_addr	WS2_32

Ci spostiamo nella sezione “**imports**” per identificare le funzione **gethostbyname** ed il suo indirizzo, ovvero **100163CC**.

La funzione si trova nella libreria WS2\_32. come indicato a destra.

### 3/4. Variabili e parametri della funzione 0x10001656

```
.text:10001656
.text:10001656 ; !!!!!!!!!!!!!!!!!!!!! SUBROUTINE !!!!!!!!!!!!!
.text:10001656
.text:10001656 ; DWORD __stdcall sub_10001656(LPVOID)
.text:10001656 sub_10001656 proc near ; DATA
.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
.text:10001656
.text:10001656 sub esp, 678h
```

Dopo aver identificato i parametri e le variabili della funzione in questione, IDA Pro assegna a loro un nome arbitrario che verrà poi utilizzato di seguito all'interno del codice assembly per facilitare l'interpretazione.

Le variabili sono quelle con il meno davanti ed i parametri senza.