

Analisi statica avanzata con IDA

ESERCIZIO

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
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?

INDIRIZZO FUNZIONE DLLMAIN

Indirizzo inizio DLLMain






```
.text:1000D02E ; BOOL __stdcall DllMain(HINSTANCE hInstDLL,DWORD fdwReason,LPVOID lpvReserved)
.text:1000D02E _DllMain@12      proc near          ; CODE XREF: DllEntryPoint+4B↓p
.text:1000D02F                ; DATA XREF: sub_1001185F+2D1↓p
```

Indirizzo Fine DDLMain

```
.text:1000D10A                retn
.text:1000D10A _DllMain@12      endp
.text:1000D10B                ;
```

FUNZIONE GETHOSTBYNAME

L'indirizzo della funzione gethostbyname è **100163CC**

	100162D8		fseek	MSVCRT
	10016278		ftell	MSVCRT
	100162A0		fwrite	MSVCRT
	100163CC	52	gethostbyname	WS2_32
	100163E4	9	htons	WS2_32

NUMERO VARIABILI E NUMERO PARAMETRI

Sappiamo che le variabili hanno valore negativo rispetto a EBP e i parametri invece hanno valore positivo; grazie a questa conoscenza possiamo facilmente contare che le **variabili sono 20** e i **parametri 1**

```
.text:10001656
.text:10001656
.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
.text:10001656
*
.text:10001656
*
.text:10001656 sub esp, 678h
*
.text:10001656
```