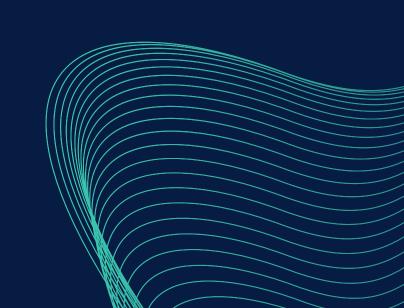


Lo scopo dell'esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l'analisi statica. A tal proposito, con riferimento al malware chiamato «Malware_U3_W3_L2» presente all'interno della cartella «Esercizio_Pratico_U3_W3_L2» sul Desktop della macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti, utilizzando IDA Pro.

- 1. Individuare l'indirizzodella funzione DLLMain(così com'è, in esadecimale)
- 2. Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l'indirizzo dell'import? Cosa fa la funzione?
- 3. Quante sono le variabili locali della funzionealla locazione di memoria 0x10001656?
- 4. Quanti sono, invece, i parametri della funzione sopra?
- 5. Inserire altre considerazioni macro livello sul malware (comportamento)

X	=	IDA	View-A	X	011	Hex	View	-A	ΧĮ	∬ SI	tructure	s :	X Er	ı En	ums	X		Imports	X 🛅	Exports	
100	00CF	EE	96	83	7D	9C	02	76	0 5	E8	5C	FA	FF	FF	FF	05	98	32	.â}	v.Þ\-	.ij2
100	30CF	FE	69	10	56	56	56	68	96	CC	99	10	56	56	FF	15	08	62		h.¦V	Ub
100																			_	bí	
																				°.uÚ_^	
																			_	.à+	_
100	3 OD 6	3E	A3	99	30	69	10	A1	44	90	01	10	56	83	CØ	ØD	57	50	ú.0:	íDÉV	â+.WP
100	3 OD 6)4E	E8	F9	7E	99	99	8B	1D	08	62	01	10	8B	35	CØ	62	91	þ"~	ïb	ï5+b.



Indirizzo esadecimale di DLLMain

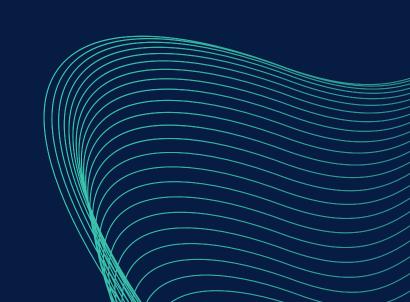
```
; BOOL __stdcall DllMain(HINSTANCE hinstDLL, |
_DllMain@12 proc near
hinstDLL= dword ntr 4
```

```
🗙 🔳 IDA View-A 💢 🔛 Hex View-A 🛛 🗙 💢 Structures 🕽 🗙 En Enums 🕽 🗙 🖼 Imports 🕽 🗙 🏥 Exports
                                                             .â}..v.Þ\·
                                                                          .ÿ2
1000CFEE
                                   00 10 56 56 FF 15 08 62
                                                             ... VV......b
1000CFFE
          09 10 56 56 56 68 06 CC
                                                             ..j. ..b..íáß..â
          01 10 6A 0A FF 15 1C 62 01 10 A1 A0 E1 08 10 83
1000D00E
         F8 03 74 05 83 F8 01 75 E9 5F 5E 5B C9 C2 08 00 ".t.â".uÚ_^[+-..
1000D01E
         8B 44 24 08 48 OF 85 CE 00 00 00 8B 44 24 04 53 TD$.H.à+...TD$.S
1000D02E
         A3 00 30 09 10 A1 44 90 01 10 56 83 C0 0D 57 50 ú.O..íDÉ..Vâ+.WP
1000D03E
1000D04E E8 F9 7E 00 00 8B 1D 08 62 01 10 8B 35 C0 62 01 þ"~..ï..b..ï5+b.
```

FUNZIONE: gethostbyname

La sua funzione principale è ottenere informazioni sulle risorse di rete, come indirizzi IP, associati a un determinato nome host

00000000100163CC	52 gethostbyname	WS2_32
INDIRIZZO	FUNZIONE	LIBRERIA



VARIABILI DELLA FUNZIONE getaddressbyhost

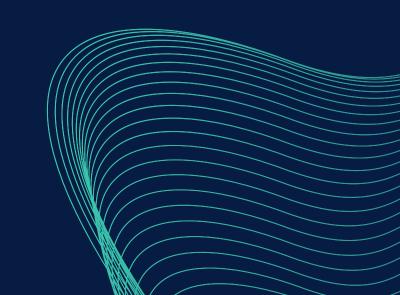
```
hLibModule= dword ptr -670h
timeout= timeval ptr -<mark>66Ch</mark>
name= sockaddr ptr -664h
var_654= word ptr -654h
Dst= dword ptr -650h
Parameter= byte ptr -644h
var_640= byte ptr -640h
CommandLine= byte ptr -63Fh
Source= byte ptr -63Dh
Data= byte ptr -638h
var 637= byte ptr -637h
var 544= dword ptr -544h
var_50C= dword ptr -50Ch
var 500= dword ptr -500h
Buf2= byte ptr -4FCh
readfds= fd set ptr -4BCh
phkResult= byte ptr -3B8h
var 380= dword ptr -380h
var_1A4= dword ptr -1A4h
var 194= dword ptr -194h
WSAData= WSAData ptr -190h
```

Le variabili sono ad un offset negativo rispetto al registro EBP e sono in totale 21

PARAMETRI

E' un argomento di una funzione o una variabile di tipo "double word" (32 bit) che si trova a un offset di 4 byte rispetto a un certo punto di riferimento.

I parametri si trovano ad un offset positivo rispetto ad EBP



Il comportamento del malware è un trojan. E tramite una backdoor può modificare file e avere informazione sugli indirizzi della macchina vittima.
parametri potrebbero essere utilizzati per stabilire una connessione con un server remoto controllato dal malware. Questo consentirebbe al malware di ricevere istruzioni da un attaccante e trasmettere informazioni dal sistema infetto
E se un malware interviene su chiamate a funzioni di sistema come CreateThread, potrebbe cercare di eseguire codice dannoso all'interno di un nuovo thread, rendendo più difficile la rilevazione e il monitoraggio da parte degli antivirus e delle soluzioni di sicurezza