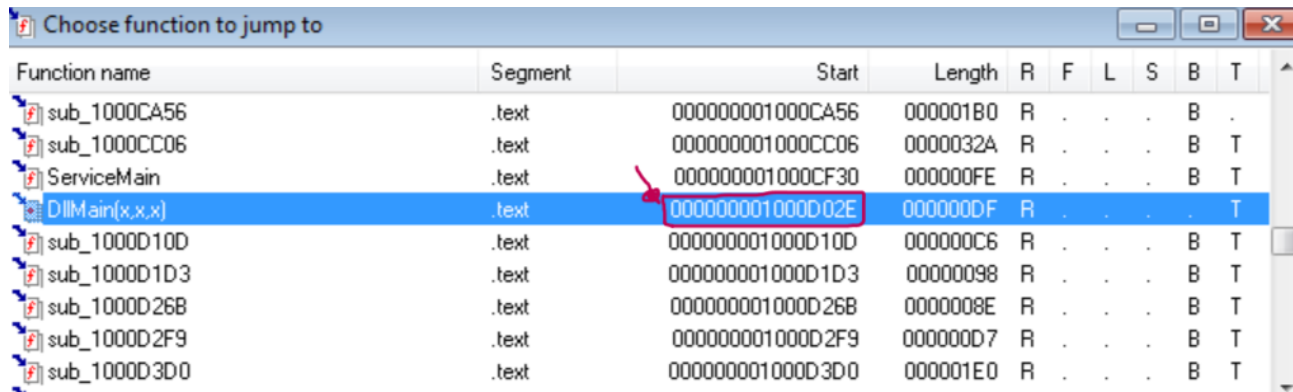


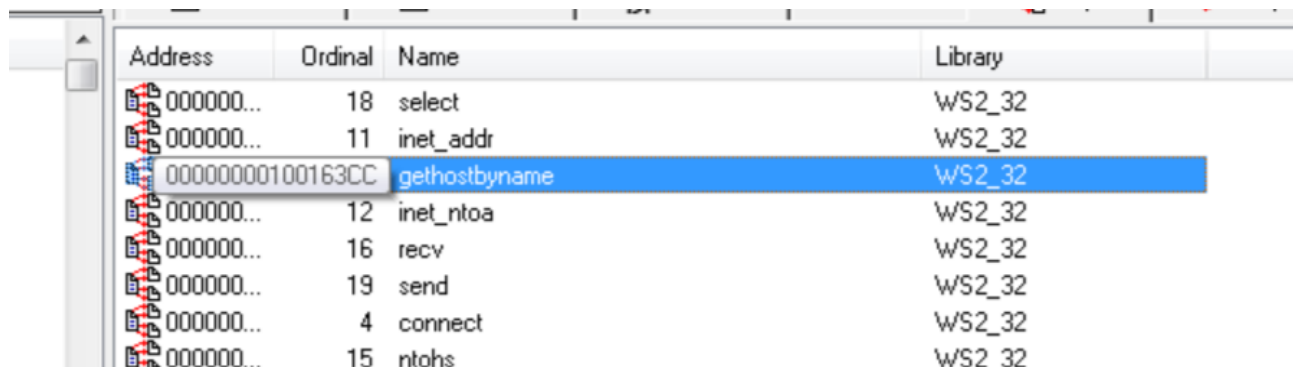
Con riferimento al malware chiamato «Malware_U3_W3_L2» presente all'interno della cartella «Esercizio_Pratico_U3_W3_L2» sul Desktop della macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti, utilizzando IDA Pro.

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



Function name	Segment	Start	Length	R	F	L	S	B	T
sub_1000CA56	.text	000000001000CA56	000001B0	R	.	.	.	B	.
sub_1000CC06	.text	000000001000CC06	0000032A	R	.	.	.	B	T
ServiceMain	.text	000000001000CF30	000000FE	R	.	.	.	B	T
DLLMain(x.x.x)	.text	000000001000D02E	000000DF	R	T
sub_1000D10D	.text	000000001000D10D	000000C6	R	.	.	.	B	T
sub_1000D1D3	.text	000000001000D1D3	00000098	R	.	.	.	B	T
sub_1000D26B	.text	000000001000D26B	0000008E	R	.	.	.	B	T
sub_1000D2F9	.text	000000001000D2F9	000000D7	R	.	.	.	B	T
sub_1000D3D0	.text	000000001000D3D0	000001E0	R	.	.	.	B	T

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



Address	Ordinal	Name	Library
00000000100163CC	18	select	WS2_32
00000000100163C8	11	inet_addr	WS2_32
00000000100163CC		gethostbyname	WS2_32
00000000100163C4	12	inet_ntoa	WS2_32
00000000100163C0	16	recv	WS2_32
00000000100163BC	19	send	WS2_32
00000000100163B8	4	connect	WS2_32
00000000100163B4	15	ntohs	WS2_32

La funzione `gethostbyname` è una funzione della libreria Winsock (Windows Sockets) utilizzata per recuperare informazioni su un host specificato dal suo nome:

struct hostent *gethostbyname(const char *name);

Questa funzione prende come parametro il nome dell'host (in formato stringa C) e restituisce un puntatore a una struttura `hostent`. Questa struttura contiene informazioni sull'host, come il suo indirizzo IP, il nome dell'host e altre informazioni correlate.

Quindi, quando chiamata, la funzione `gethostbyname` cerca l'host specificato dal nome fornito e restituisce un puntatore alla struttura `hostent` che contiene le informazioni richieste.

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

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

Nella funzione sub_10001656 fornita, possiamo identificare le seguenti variabili locali e parametri:

- **Parametri:**

arg_0 (DWORD ptr 4): Questo è un parametro della funzione che viene passato attraverso lo stack.

- **Variabili locali:**

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 (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_3B0 (dword ptr -3B0h)

var_1A4 (dword ptr -1A4h)

var_194 (dword ptr -194h)

WSAData (WSAData ptr -190h)

Quindi, ci sono **1 parametro** (arg_0) e **24 variabili locali** nella funzione sub_10001656.

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

Si potrebbe trattare di un malware che va ad effettuare un'escalation dei privilegi. Utilizza la funzione `gethostbyname` per ottenere informazioni.