

S11/L2

Traccia:

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(così com'è, in esadecimale)

Andiamo su “Open name windows” e cerchiamo la funzionea DllMain con il seguente indirizzo esadecimale: **1000D02E**

Name	Address	P.
PSLIST	0000000010007025	P
nullsub_1	000000001000706F	
nullsub_2	000000001000707C	
StartEXS	0000000010007ECB	P
HandlerProc	000000001000C9DF	
ServiceMain	000000001000CF30	P
DllMain(x,x,x)	000000001000D02E	
InstallRT	000000001000D847	P
InstallSA	000000001000DEC1	P
InstallSB	000000001000E892	P
UninstallSA	000000001000EA05	P
UninstallSB	000000001000F138	P
UninstallRT	000000001000F405	P
StartAddress	0000000010010740	
GetModuleFileNameExA	00000000100111A6	
EnumProcessModules	00000000100111AC	

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

Da “imports” individuiamo la seguente funzione: gethostbyname. Il suo indirizzo è: **100163CC**

Address	Ordinal	Name	Library
00000000100163C4	18	select	WS2_32
00000000100163C8	11	inet_addr	WS2_32
00000000100163CC	52	gethostbyname	WS2_32
00000000100163D0	12	inet_ntoa	WS2_32
00000000100163D4	16	recv	WS2_32
00000000100163D8	19	send	WS2_32
00000000100163DC	4	connect	WS2_32
00000000100163E0	15	ntohs	WS2_32
00000000100163E4	9	htons	WS2_32
00000000100163E8	21	setsockopt	WS2_32
00000000100163EC	116	WSACleanup	WS2_32
00000000100163F0	115	WSAStartup	WS2_32
00000000100163F4	3	closesocket	WS2_32
00000000100163F8	23	socket	WS2_32
00000000100163FC	111	WSAGetLastError	WS2_32
0000000010016404		GetAdaptersInfo	iphlpapi

La funzione "gethostbyname" è una funzione di sistema utilizzata per ottenere l'indirizzo IP associato a un nome host. In pratica, accetta il nome dell'host come parametro e restituisce un puntatore a una struttura che contiene informazioni sull'host, incluso il suo indirizzo IP.

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

Andiamo su "Hex view" e trascriviamo la nostra allocazione di memoria: 10001656, dopo di che, vediamo la corrispondenza su "IDA view-A".

**Le variabili** sono ad un offset (differenza rispetto ad un valore) negativo rispetto al registro EBP; per cui come vediamo esse sono **23**:

```
sub_10001656 proc near
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
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
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
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
arg_0= dword ptr 4
sub esp, 678h
push ebx
push ebp
```

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

**I parametri** invece, ovvero quelli che si trovano ad un offset positivo rispetto ad EBP, in questo caso **sono 1** ovvero l'ultima riga:

arg\_0= dword ptr 4

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

Nel contesto dell'analisi di un malware all'interno di IDA Pro, individuare la funzione "gethostbyname" potrebbe indicare che il malware sta cercando di comunicare con un server remoto tramite il nome dell'host anziché l'indirizzo IP diretto. Questo può essere un indicatore che il malware sta cercando di contattare un server remoto per scopi come l'invio di dati rubati, ricezione di comandi o altri scopi maligni legati alla comunicazione in rete. Possiamo dunque ipotizzare che si tratti di una backdoor, in quanti sono progettati per consentire l'accesso remoto non autorizzato al sistema infetto.