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)
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 funzione alla locazione di memoria 0x10001656?
4. Quanti sono, invece, i parametri della funzione sopra?
5. Inserire altre considerazioni macro livello sul malware (comportamento).

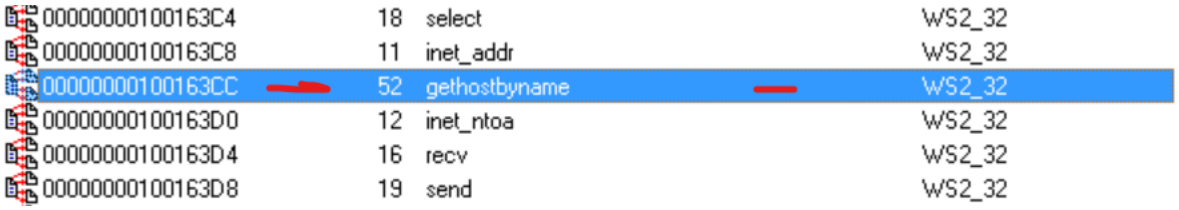
INDIRIZZO DELLA FUNZIONE

L'indirizzo della funzione è **1000D02E .**

IMPORT

La funzione gethostbyname è quella in blu e il suo indirizzo è nella prima colonna partendo da sinistra ed è **000000001001163CC.**

La funzione **gethostbyname** recupera le informazioni host corrispondenti a un nome host da un database host.



VARIABILI LOCALI E PARAMETRI

Le variabili e i parametri sono tutte le righe contenenti le scritte in verde tranne l'ultima.
L'ultima riga è un parametro in quanto ha un offset positivo.

```
; DWORD __stdcall sub_10001656(LPVOID)
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
Paraneter= 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
arg_0= dword ptr  4
```

COMPORTAMENTO DEL MALWARE

Il malware tenta di aprire una backdoor sul pc vittima. Questo può essere dedotto dal fatto che contiene sia le funzioni di invio (send) che di ricezione (recv). Inoltre, si nota che il malware stabilisce una connessione all'avvio, il che suggerisce che tenga traccia dei dati e delle azioni dell'utente.