

Pratica 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)

IDA (Interactive Disassembler) è un disassembler usato per il reverse engineering e supporta numerosi formati di file eseguibili per diversi processori e sistemi operativi.

1. Individuare l'indirizzo della funzione DLLMain

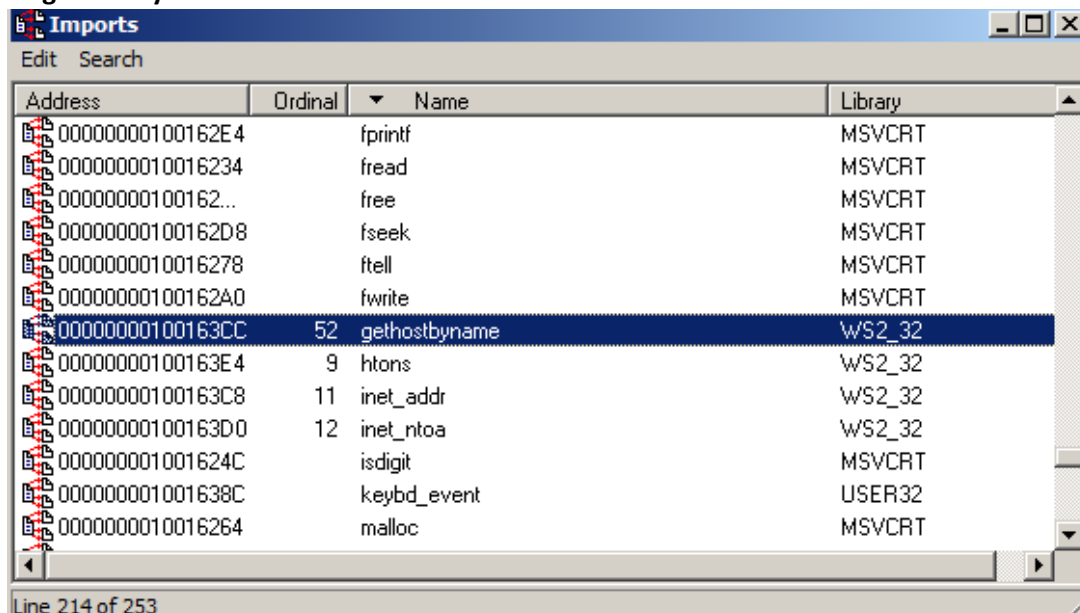
Dopo aver avviato IDA e caricato il file, per poter individuare l'indirizzo della funzione DLLMain abbiamo premuto immediatamente la barra spaziatrice, così da avere la modalità testuale del file.

```
.text:1000D02E ; ===== S U B R O U T I N E =====
.text:1000D02E
.text:1000D02E
.text:1000D02E ; 800L stdcall DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
.text:1000D02E DllMain@12 proc near ; CODE XREF: DllEntryPoint+4B↓p
.text:1000D02E ; DATA XREF: sub_100110FF+2D↓o
.text:1000D02E
.text:1000D02E hinstDLL = dword ptr 4
```

Così facendo è stato trovato l'indirizzo della funzione DLLMain **1000D02E**

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

Per trovare l'indirizzo dell'imports ho ordinato in modo crescente la scheda imports riuscendo a trovare l'indirizzo della funzione «**gethostbyname**» **100163CC**.

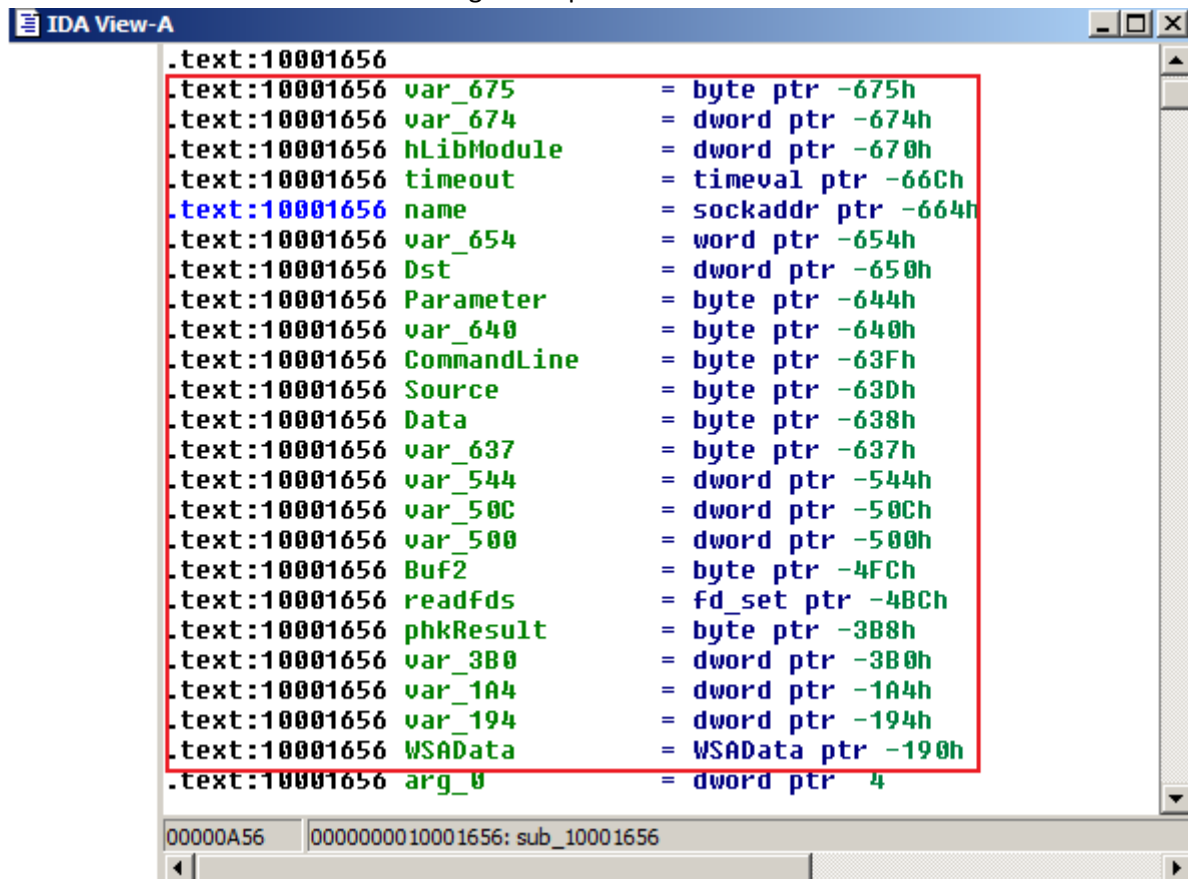


La funzione «**gethostbyname**» non può accettare una stringa di indirizzo IP come parametro passato al nome e risolverla in un nome host. Questa richiesta viene considerata come una rappresentazione di stringa di un indirizzo IPv4 o viene passato un nome host sconosciuto.

Usa la funzione WSALookupServiceBegin (una query client che restituisce solo un handle usato dalle chiamate successive per ottenere risultati effettivi) per eseguire query della classe di servizio.

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

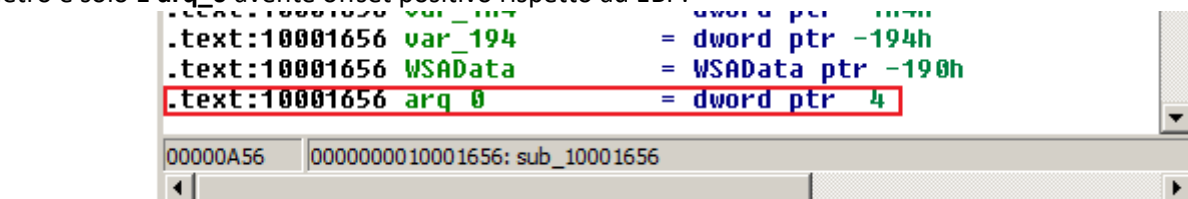
Dal menù di IDA è stato selezionato Jump->Jump Address per poter essere indirizzato alla locazione di memoria 10001656 trovando **23** variabili aventi offset negativi rispetto ad EBP



```
.text:10001656
.text:10001656 var_675      = byte ptr -675h
.text:10001656 var_674      = dword ptr -674h
.text:10001656 hLibModule    = dword ptr -670h
.text:10001656 timeout      = timeval ptr -66Ch
.text:10001656 name         = sockaddr ptr -664h
.text:10001656 var_654      = word ptr -654h
.text:10001656 Dst          = dword ptr -650h
.text:10001656 Parameter    = byte ptr -644h
.text:10001656 var_640      = byte ptr -640h
.text:10001656 CommandLine  = byte ptr -63Fh
.text:10001656 Source       = byte ptr -63Dh
.text:10001656 Data         = byte ptr -638h
.text:10001656 var_637      = byte ptr -637h
.text:10001656 var_544      = dword ptr -544h
.text:10001656 var_50C      = dword ptr -50Ch
.text:10001656 var_500      = dword ptr -500h
.text:10001656 Buf2         = byte ptr -4FCh
.text:10001656 readfds      = fd_set ptr -4BCh
.text:10001656 phkResult    = byte 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
```

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

Il parametro è solo 1 **arg_0** avente offset positivo rispetto ad EBP.



```
.text:10001656 var_194      = dword ptr -194h
.text:10001656 WSAData      = WSADATA ptr -190h
.text:10001656 arg_0        = dword ptr 4
```

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

Il malware tenta di creare un host all'interno del sistema operativo utilizzando la funzione «**gethostbyname**».