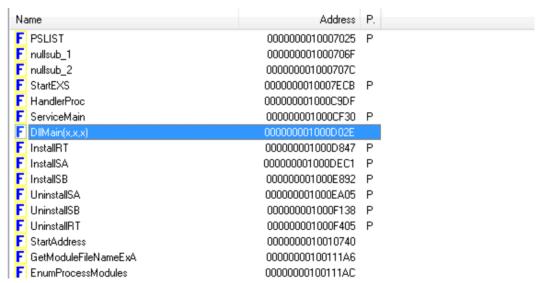
S11/L2

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.

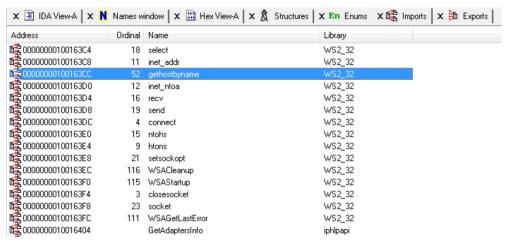
1. Individuare l'indirizzo della funzione DLLMain(così com'è, in esadecimale)

Andiamo su "Open name windows" e cerchiamo la funziona DllMain con il seguente indirizzo esadecimale: **1000D02E**



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**



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:

```
var 640= byte ptr -640h
sub 10001656 proc near
                                         CommandLine= byte ptr -63Fh
                                         Source= byte ptr -63Dh
var 675= byte ptr -675h
                                         Data= byte ptr -638h
var_674= dword ptr -674h
                                         var 637= byte ptr -637h
hLibModule= dword ptr -670h
                                         var_544= dword ptr -544h
timeout= timeval ptr -66Ch
                                         var_50C= dword ptr -50Ch
name= sockaddr ptr -664h
                                         var_500= dword ptr -500h
var_654= word ptr -654h
                                         Buf2= byte ptr -4FCh
Dst= dword ptr -650h
                                         readfds= fd set ptr -4BCh
Parameter= byte ptr -644h
                                         phkResult= byte ptr -3B8h
var 640= byte ptr -640h
                                         var 3B0= dword ptr -3B0h
CommandLine= byte ptr -63Fh
                                         var 1A4= dword ptr -1A4h
Source= byte ptr -63Dh
                                         var_194= dword ptr -194h
Data= byte ptr -638h
                                         WSAData= WSAData ptr -190h
var_637= byte ptr -637h
var_544= dword ptr -544h
var_50C= dword ptr -50Ch
                                         arg 0= dword ptr 4
var_500= dword ptr -500h
                                                 esp, 678h
Buf2= byte ptr -4FCh
                                         push
                                                 ebx
readfds= fd set ptr -4BCh
                                                 ebo
```

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

I parametri invece, ovvero quelli che si trovano 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.