Report Esercizio

W23-D5

Redatto da Andrea Sciattella

29/07/2024

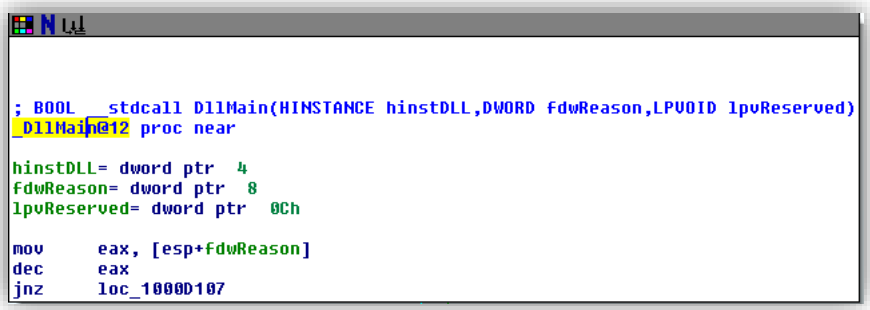
TRACCIA

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.

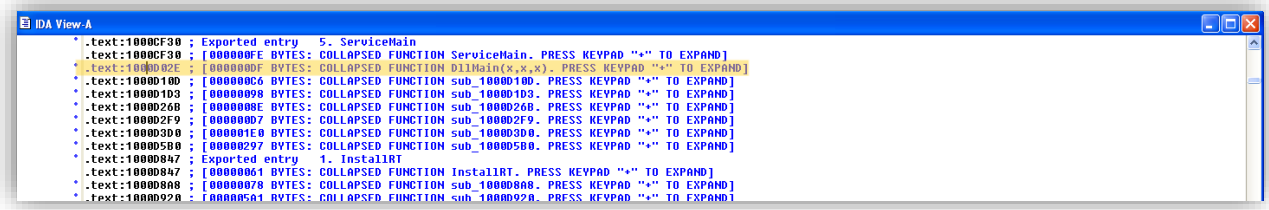
1. Individuare l'indirizzo della funzione DLLMain (così com'è, in esadecimale)
2. Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l'indirizzo dell'import?
3. Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656?
4. Quanti sono, invece, i parametri della funzione sopra?
5. Inserire altre considerazioni macro-livello sul malware

SVOLGIMENTO ESERCIZIO

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

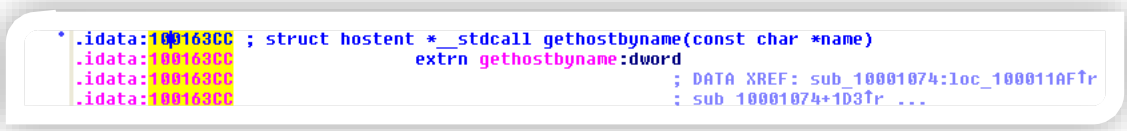


- Abbiamo trovato la parte menzionata della funzione "*DLLMain*" tramite la ricerca, ora premiamo la barra spaziatrice per passare alla visuale testuale.



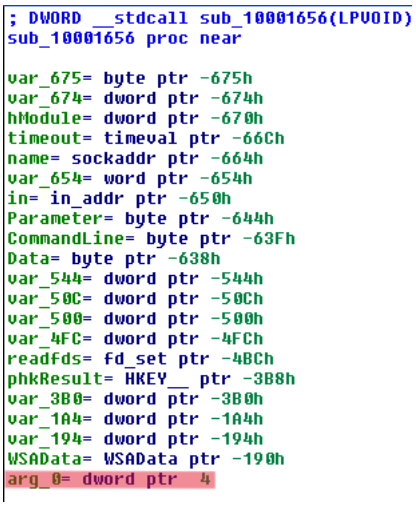
- L'indirizzo in esadecimale della funzione "*DLLMain*" è **.text:1000D02E**

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



- Come possiamo vedere dallo screenshot, l'indirizzo della funzione è **.text:100163CC**

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



```
; DWORD __stdcall sub_10001656(LPVOID)
sub_10001656 proc near

var_675= byte ptr -675h
var_674= dword ptr -674h
hModule= dword ptr -670h
timeout= timeval ptr -66Ch
name= sockaddr ptr -664h
var_654= word ptr -654h
in= in_addr ptr -650h
Parameter= byte ptr -644h
CommandLine= byte ptr -63Fh
Data= byte ptr -638h
var_544= dword ptr -544h
var_50C= dword ptr -50Ch
var_500= dword ptr -500h
var_4FC= dword ptr -4FCh
readfds= fd_set ptr -4BCh
phkResult= HKEY__ 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
```

- La funzione ha come variabili locali tutti i valori che hanno offset negativo, e nel nostro caso ne abbiamo **20**.

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

- Guardando sempre nello screen precedente, troviamo 1 sola informazione con valore positivo evidenziata di rosso, "***arg_0***"