

CS0124

REPORT

PROGETTO

S11L2

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.

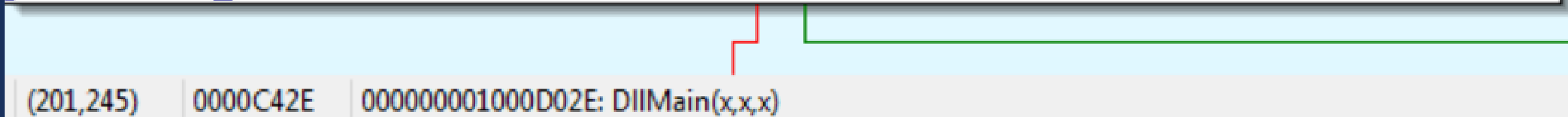
- 1. Individuare l'indirizzo della funzione DLLMain(così com'è, in esadecimale)**
- 2. Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l'indirizzo dell'import? Cosa fa la funzione?**
- 3. Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656?**
- 4.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

Prima consegna

```
; BOOL __stdcall DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
_DllMain@12 proc near

hinstDLL= dword ptr  4
fdwReason= dword ptr  8
lpvReserved= dword ptr 0Ch

mov     eax, [esp+fdwReason]
dec     eax
jnz     loc_1000D107
```



(201,245) | 0000C42E | 000000001000D02E: DllMain(x,x,x)

Qui individuiamo l'indirizzo della funzione Dllmain,
come possiamo vedere in figura troviamo anche il
valore in esadecimale 1000D02E

Seconda consegna

La funzione gethostbyname e' utilizzata dal malware per identificare l'indirizzo ip dell'end point dopo aver eseguito il file.

Terza consegna

.text:10001656	var_675	= byte ptr -675h	10001656	var_500	= dword ptr -500h
.text:10001656	var_674	= dword ptr -674h	10001656	Buf2	= byte ptr -4FCh
.text:10001656	hLibModule	= dword ptr -670h	10001656	readfds	= fd_set ptr -4BCh
.text:10001656	timeout	= timeval ptr -66Ch	10001656	phkResult	= byte ptr -3B8h
.text:10001656	name	= sockaddr ptr -664h	10001656	var_3B0	= dword ptr -3B0h
.text:10001656	var_654	= word ptr -654h	10001656	var_1A4	= dword ptr -1A4h
.text:10001656	Dst	= dword ptr -650h	10001656	var_194	= dword ptr -194h
.text:10001656	Parameter	= byte ptr -644h	10001656	WSAData	= WSAData ptr -190
.text:10001656	var_640	= byte ptr -640h	10001656	arg_0	= dword ptr 4
.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			

L'unico parametro presente e' arg_0 ptr 4

Come possiamo vedere le variabili locali
all'interno della funzione sono 23

Grazie!