MALWARE ANALYSIS

ANALISI STATICA AVANZATA CON IDA

TRACCIA

Lo scopo dell'esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l'a n a lis i s t a t ic a . 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 PRO

IDA è un disassembler interattivo e debugger usato principalmente per l'analisi del software a livello binario. Sviluppato da Hex-Rays, IDA Pro è uno strumento potente e versatile utilizzato da ingegneri del software, analisti di sicurezza e ricercatori per esplorare e comprendere il funzionamento interno di programmi eseguibili.

Le principali caratteristiche di IDA Pro sono:

1. **Disassemblaggio Interattivo:** IDA Pro trasforma il codice macchina in un formato leggibile (assembly), permettendo agli utenti di esplorare il flusso di esecuzione del programma.
2. **Supporto Multiarchetetturale:** Supporta un'ampia gamma di architetture di processore, incluse x86, x64, ARM, PowerPC e molte altre.
3. **Debugger Integrato:** Permette di eseguire il codice in tempo reale per analizzare il comportamento dinamico del software, identificare bug e vulnerabilità.
4. **Analisi Automatica e Manuale:** IDA Pro combina tecniche di analisi automatica con la possibilità di intervento manuale per migliorare la precisione del disassemblaggio.
5. **Scriptabilità**: Supporta scripting in Python e IDC (IDA Scripting Language) per automatizzare compiti ripetitivi e personalizzare l'analisi.

IDA Pro è uno strumento essenziale nella cassetta degli attrezzi di chiunque si occupi di reverse engineering, analisi di malware e analisi forense del software.

Indirizzo funzione DDLmain

```
.text:1000D02E ; ============== S U B R O U T I N E =======================================
.text:1000D02E
.text:1000D02E
.text:1000D02E ; BOOL __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
.text:1000D02E fdwReason       = dword ptr  8
.text:1000D02E lpvReserved     = dword ptr  0Ch
.text:1000D02E
.text:1000D02E                 mov     eax, [esp+fdwReason]
```

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

Si riferisce alla posizione specifica nella memoria di un computer dove si trova il codice eseguibile di quella funzione.

Gethostbyname

Idirizzo

Dalla sezione imports del software, notiamo che l'indirizzo è: **100163CC**

Cosa fa

La funzione gethostbyname è una funzione della libreria di rete standard che viene utilizzata per risolvere i nomi di host (come "www.example.com") in indirizzi IP. Essa è parte della libreria di rete dei sistemi operativi basati su Unix e Windows

Variabili della locazione di memoria 10001656

Le variabili che troviamo a questo indirizzo di memoria sono 20

```
.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
```

Argomenti della locazione di memoria 10001656

A questo indirizzo di memoria troviamo un unico argomento “arg_0”

```
.text:10001656 arg_0                   = dword ptr  4
```