Aguglia Andrea

Analisi statica avanzata con IDA

Cyber Security & Ethical Hacking

Traccia

Traccia:

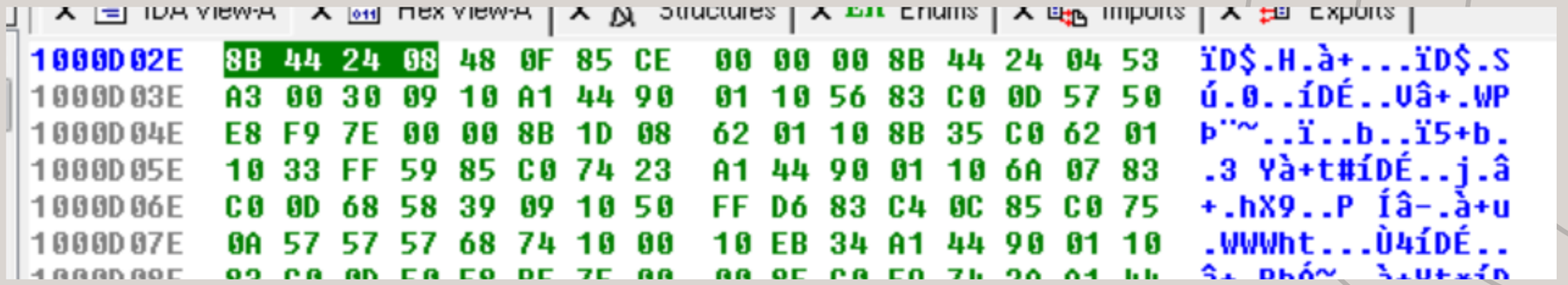
Lo scopo dell'esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l'analisi statica.
A tal proposito, con riferimento al malware chiamato «**Malware_U3_W3_L2** » presente all'interno della cartella «**Esercizio_Pratico_U3_W3_L2** » sul Desktop della macchina virtuale dedicata 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)

1


IDA View-A
Hex View-A
Structures
Enums
Imports
Exports
1000D02E 8B 44 24 08 48 0F 85 CE 00 00 00 8B 44 24 04 53 ïD$.H.à+...ïD$.S
1000D03E A3 00 30 09 10 A1 44 90 01 10 56 83 C0 0D 57 50 ú.0..ÍDÉ..Vâ+.WP
1000D04E E8 F9 7E 00 00 8B 1D 08 62 01 10 8B 35 C0 62 01 Þ¨~..ï..b..ï5+b.
1000D05E 10 33 FF 59 85 C0 74 23 A1 44 90 01 10 6A 07 83 .3 Yà+t#ÍDÉ..j.â
1000D06E C0 0D 68 58 39 09 10 50 FF D6 83 C4 0C 85 C0 75 +.hX9..P Íâ-.à+u
1000D07E 0A 57 57 57 68 74 10 00 10 EB 34 A1 44 90 01 10 .WWWht...Ù4ÍDÉ..

2

```
.idata:100163C4                                         ; DATA XREF: sub_10001656+3D2↑r ...
.idata:100163C8 ; unsigned __int32 __stdcall inet_addr(const char *cp)
.idata:100163C8                 extrn inet_addr:dword   ; CODE XREF: sub_10001074+11E↑p
.idata:100163C8                                         ; sub_10001074+1BF↑p ...
.idata:100163CC ; struct hostent *__stdcall gethostbyname(const char *name)
.idata:100163CC                 extrn gethostbyname:dword
.idata:100163CC                                         ; CODE XREF: sub_10001074:loc_100011AF↑p
.idata:100163CC                                         ; sub_10001074+1D3↑p ...
.idata:100163D0 ; char *__stdcall inet_ntoa(struct in_addr in)
.idata:100163D0                 extrn inet_ntoa:dword   ; CODE XREF: sub_10001074:loc_10001311↑p
.idata:100163D0                                         ; sub_10001365:loc_10001602↑p ...
.idata:100163D4 ; int __stdcall recv(SOCKET s, char *buf, int len, int flags)
.idata:100163D4                 extrn recv:dword        ; CODE XREF: sub_10001656+2D5↑p
.idata:100163D4                                         ; sub_10001656+3F2↑p
```

La funzione gethostbyname è una funzione di programmazione utilizzata per ottenere informazioni su un host utilizzando il suo nome. Di solito, viene utilizzata per ottenere l'indirizzo IP associato a un determinato nome host.

3

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

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

Le variabili locali della funzione alla locazione di memoria 0x10001656 sono 23

4

```
var_194= dword ptr -194h
WSAData= WSAData ptr -190h
arg_0= dword ptr  4
```

Il malware sembrerebbe un Trojan.
Un "Trojan" o "Trojan Horse" (Cavallo di Troia) è un tipo di malware (software dannoso) che si presenta come un programma legittimo o benigno ma, in realtà, svolge funzioni dannose una volta che è stato eseguito o installato sul sistema dell'utente senza il suo consenso. Il termine deriva dall'antica storia del cavallo di legno utilizzato dai Greci durante la guerra di Troia per infiltrarsi nella città nemica.

5