S11L2

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

```
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
```

L'indirizzo della funzione è 1000D02E

Traccia: Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l'indirizzo dell'import? Cosa fa la funzione?

L'indirizzo è 00000000100163CC.
La funzione gethostbyname() è una funzione di sistema disponibile in molti linguaggi di programmazione, inclusi C e C++. Questa funzione è utilizzata per ottenere informazioni sulle macchine ospiti (host) tramite il loro nome. In pratica, dato un nome di host come parametro di input, la funzione restituisce una struttura contenente informazioni sulle corrispondenti macchine.

Traccia: Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656?

```
.text:10001656 var_675         = byte ptr -675h
.text:10001656 var_674         = dword ptr -674h
.text:10001656 hLibModule      = dword ptr -670h
.text:10001656 timeout         = timeval ptr -66Ch
.text:10001656 name            = sockaddr ptr -664h
.text:10001656 var_654         = word ptr -654h
.text:10001656 Dst             = dword ptr -650h
.text:10001656 Parameter       = byte ptr -644h
.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
```

Alla locazione di memoria specificata ci sono 23 variabili locali.

Traccia: Quanti sono, invece, i parametri della funzione sopra?

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

La funzione ha solo 1 parametro.

Traccia: Inserire altre considerazioni macro livello sul malware (comportamento).
Secondo il mio parere si tratta di un malware che va a fare un’escalation dei privilegi.Inoltre una volta ottenuto l’indirizzo ip tramite la funzione gethostbyname,il programma può utilizzare quell’indirizzo per creare una connessione di rete con la vittima e quindi può connettersi ad un server per scaricare altri programmi malevoli (downloader),oppure semplicemente caricare alcuni dati sensibili rubati.