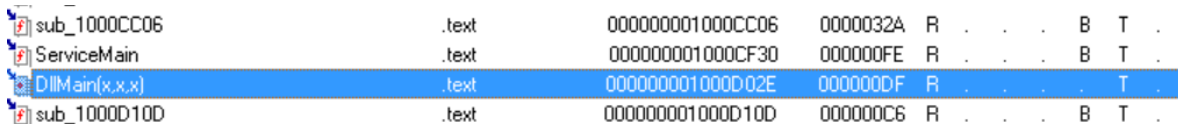
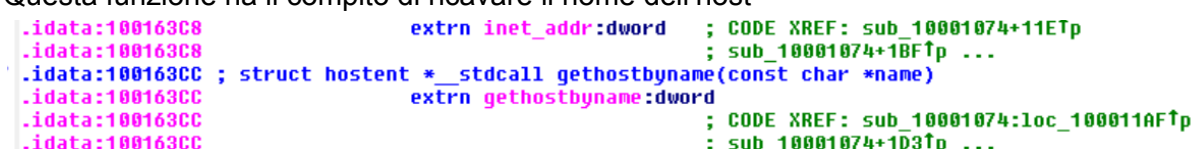


Traccia: Lo scopo dell'esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l'analisi statica. A tal proposito, con riferimento al malware chiamato «Malware_U3_W3_L2» presente all'interno della cartella «Esercizio_Pratico_U3_W3_L2» sul Desktop della macchina virtuale dedicata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


Soluzione:

1. 

Name	Address	Size	Class	Comment
sub_1000CC06	000000001000CC06	0000032A	R	
ServiceMain	000000001000CF30	000000FE	R	
DLLMain(x.x.x)	000000001000D02E	000000DF	R	
sub_1000D10D	000000001000D10D	000000C6	R	
2. Questa funzione ha il compito di ricavare il nome dell'host


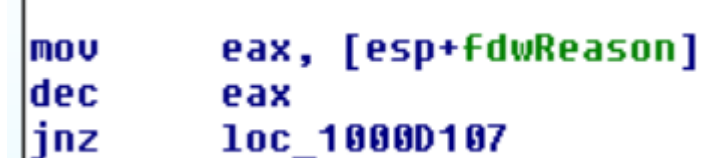
```

.idata:100163C8      extrn inet_addr:dword      ; CODE XREF: sub_10001074+11E7p
.idata:100163C8      ; sub_10001074+1BF7p ...
.idata:100163CC ; struct hostent * __stdcall gethostbyname(const char *name)
.idata:100163CC      extrn gethostbyname:dword
.idata:100163CC      ; CODE XREF: sub_10001074:loc_100011AF7p
.idata:100163CC      : sub_10001074+1D37p ...

```
3. 

```

sub     esp, 678h

```
4. 

```

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

```

5. Obiettivi del malware: IL malware può avere una vasta gamma di obiettivi, che vanno dal furto di dati e informazioni personali alla distruzione di file e sistemi, dallo spionaggio industriale alla creazione di reti botnet per attività illegali come il phishing e l'invio di spam.
6. Metodi di propagazione: I malware possono diffondersi attraverso una varietà di metodi, tra cui allegati email dannosi, link a siti web infetti, software pirata, exploit di vulnerabilità nel software e persino tramite dispositivi USB infetti.
7. Persistenza e nascita: Una volta che un malware infetta un sistema, può cercare di persistere nel tempo attraverso varie tecniche, come l'installazione di backdoor, l'iniezione di codice in processi legittimi o la modifica delle impostazioni di avvio del sistema operativo per essere eseguito automaticamente all'avvio.
8. Camuffamento e evasione: I creatori di malware spesso cercano di mascherare il proprio codice per sfuggire alla rilevazione da parte degli antivirus e degli strumenti di sicurezza. Possono utilizzare tecniche come

l'impiego di packer, l'offuscamento del codice o la modifica costante delle firme per rendere più difficile la sua identificazione.

9. Attivazione a distanza: Alcuni malware rimangono inattivi o "dormienti" all'interno di un sistema fino a quando non vengono attivati da un comando esterno. Questo può avvenire attraverso canali di comando e controllo remoti, che consentono agli attaccanti di impartire istruzioni al malware una volta che è stato distribuito.
10. Danno potenziale: I malware possono causare danni significativi ai sistemi e alle organizzazioni colpite. Questo può includere perdita di dati, interruzioni operative, danni alla reputazione aziendale e, in alcuni casi, perdite finanziarie dirette.
11. Impatto sociale ed economico: L'aumento delle minacce informatiche può avere conseguenze significative a livello sociale ed economico. Le organizzazioni possono subire perdite finanziarie a causa di interruzioni dei servizi, mentre i cittadini possono essere vittime di frodi finanziarie o furto di identità.
12. Evoluzione e adattamento: I malware continuano a evolversi in risposta alle nuove tecnologie e alle contromisure di sicurezza. Gli autori di malware cercano costantemente nuovi modi per aggirare le difese informatiche e sfruttare le vulnerabilità emergenti.

Considerando queste e altre variabili, è evidente che la lotta contro i malware richiede un approccio olistico che comprenda la prevenzione, il rilevamento e la risposta rapida agli attacchi.