EPICODE-CS0124
S11/L2 - Pratica

Flaviano Sedici

Indice

Riferimenti e versioni

Responsabile del documento: Flaviano Sedici

Versionamento

Versione	Descrizione	Riferimento	Data
1.0	Redazione documento	Responsabile	03/04/2024

1. Traccia

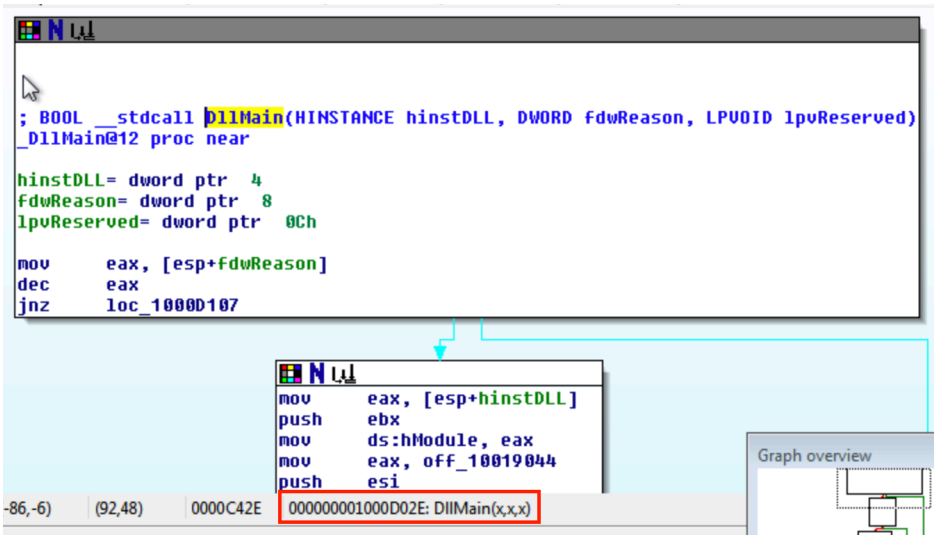
Lo scopo dell'esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l'analisi statica.

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.

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

1.1. Individuare l'indirizzo della DLLMain

Tramite la funzione di ricerca del software IDA, abbiamo recuperato la posizione della funzione DLL main locata all'indirizzo **1000D022E**.



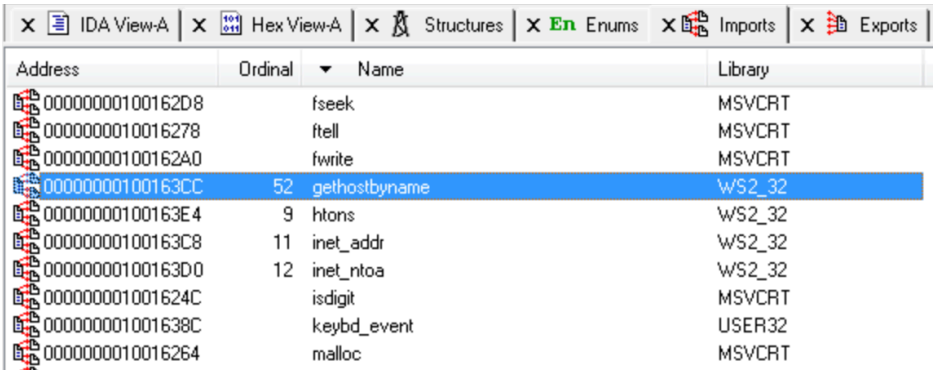
Ricerca DLLMain

1.2. gethostbyname

gethostbyname è una funzione di libreria utilizzata per ottenere informazioni sul nome host associato a un determinato indirizzo IP. È una funzione di vecchia generazione e non raccomandata per l'uso in ambienti moderni, poiché è stata sostituita da versioni più recenti e più sicure come **getaddrinfo**.

Anche in questo caso effettuiamo una ricerca testuale che ci restituisce l'indirizzo della funzione:

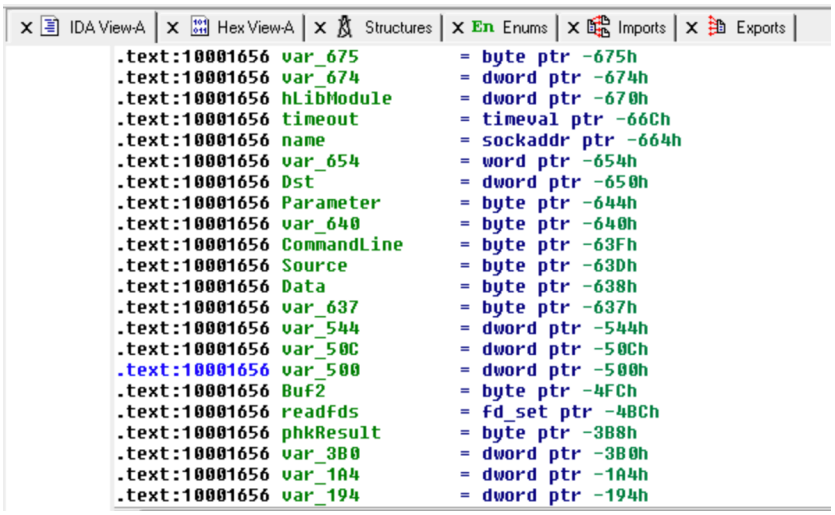
1001163C



Indirizzo funzione gethostbyname

1.3. Enumerazione variabili locali

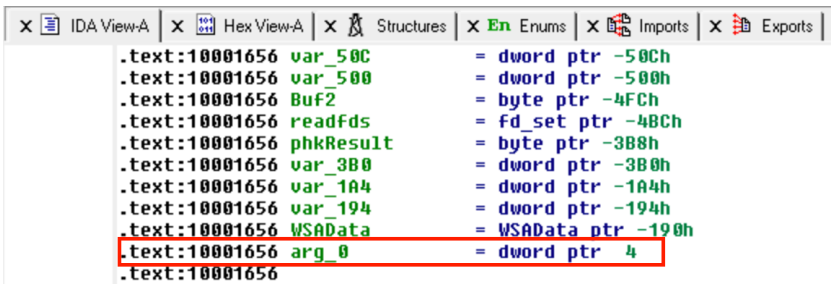
Dall'analisi effettuata è emerso che le variabili locali, ovvero le variabili con un offset negativo sono in totale 23.



Variabili locali con offset negativo

1.4. Enumerazione parametri

Dall'analisi effettuata è emerso che i parametri, ovvero le variabili con un offset positivo sono in totale 1.



Parametri con offset positivo

1.5. Comportamento del malware

Analizzando la tipologia di librerie importate e la loro numerosità, nonché la sua estensione, possiamo dedurre che sia un trojan/backdoor che contiene al suo interno una reverse shell.

La supposizione viene confermata da Virus Total che nella sezione Behavior elenca una serie di funzionalità utili all'esecuzione di comandi all'interno del target, tra cui: ricevere e inviare informazioni, effettuare screenshot, creare socket, etc.

Tutti questi tool sono dedicati al mantenimento della persistenza nell'ottica del C2 (command & control).

Riferimento Virus Total

Module Name	Imports
000158A2	N/A
szAnsi	(nFunctions)
GDI32.dll	17
PSAPI.DLL	2
WS2_32.dll	15
iphlpapi.dll	1
KERNEL32.dll	89
USER32.dll	26
ADVAPI32.dll	32
ole32.dll	5
OLEAUT32.dll	2
MSVFW32.dll	5
WINMM.dll	7
MSVCRT.dll	52

Librerie importate