

EPICODE-CS0124

S11/L2 - Pratica

Flaviano Sedici

Indice

1. Traccia	3
1.1. Individuare l'indirizzo della DLLMain	4
1.2. gethostbyname	4
1.3. Enumerazione variabili locali.....	5
1.4. Enumerazione parametri	5
1.5. Comportamento del malware.....	6

Riferimenti e versioni

Responsabile del documento: Flaviano Sedici

Versionamento

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

1. Traccia

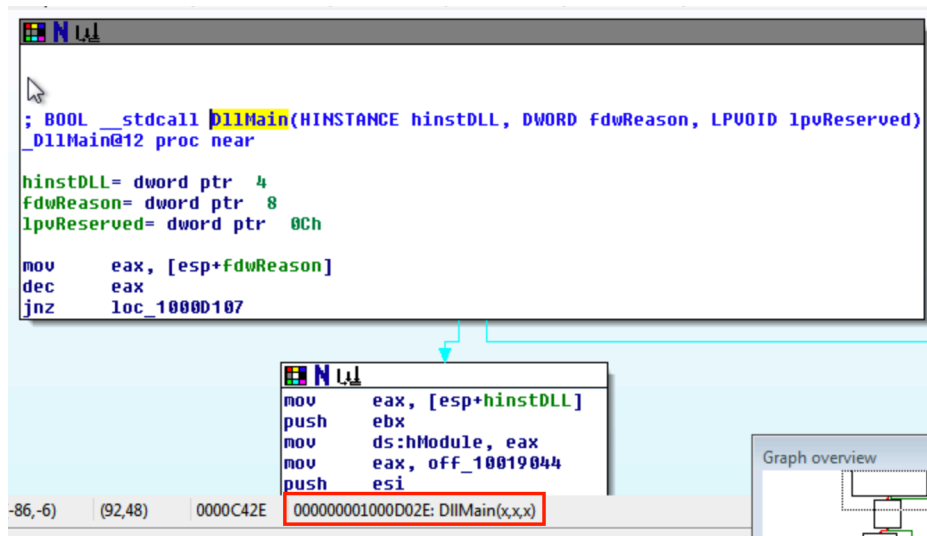
Lo scopo dell'esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l'analisi statica.

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

Address	Ordinal	Name	Library
00000000100162D8		fseek	MSVCRT
0000000010016278		ftell	MSVCRT
00000000100162A0		fwrite	MSVCRT
00000000100163CC	52	gethostbyname	WS2_32
00000000100163E4	9	htons	WS2_32
00000000100163C8	11	inet_addr	WS2_32
00000000100163D0	12	inet_ntoa	WS2_32
000000001001624C		isdigit	MSVCRT
000000001001638C		keybd_event	USER32
0000000010016264		malloc	MSVCRT

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.

.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

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.

.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
.text:10001656		

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