REPORT

2024

PREPARED BY
PHANTOM SRL

INDICE

Page 3: Traccia

Page 4: Funzione DLL Main

Page 5: GetHostByName

Page 6: Variabili Locali

Page 7: Parametri Presenti

TRACCIA

Traccia:

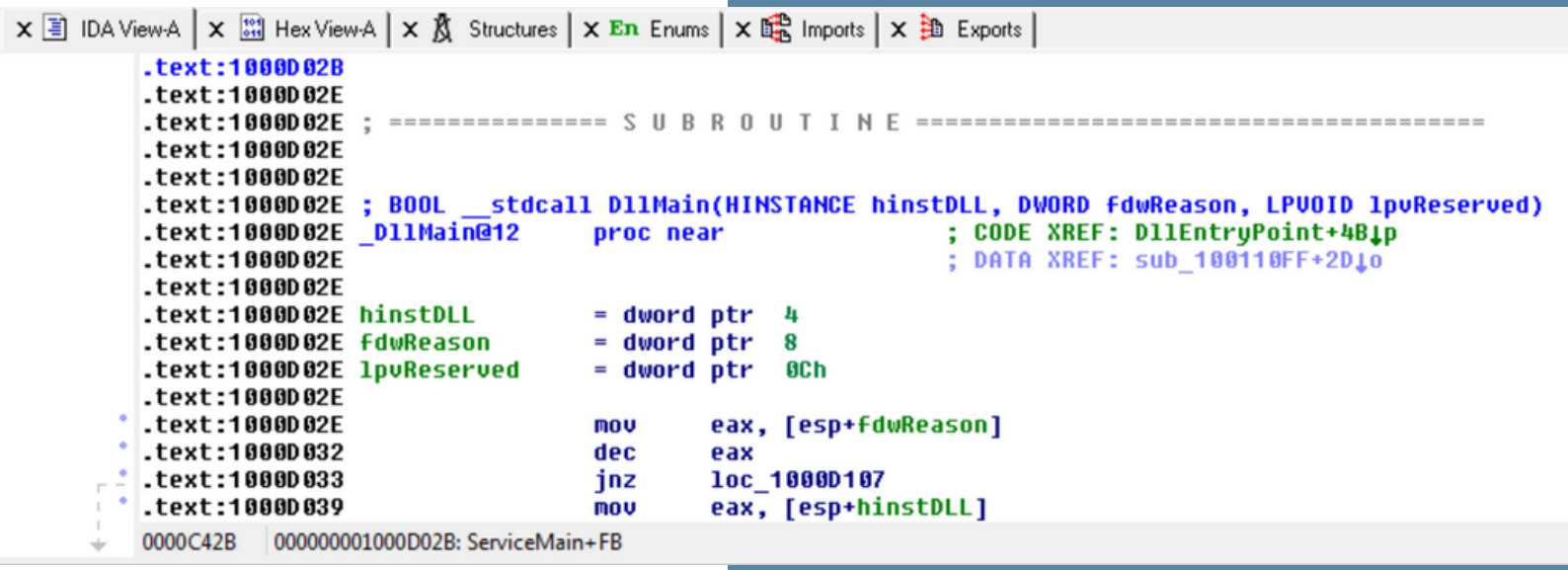
Lo scopo dell'esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l'analisi statica.
A tal proposito, con riferimento al malware chiamato «**Malware_U3_W3_L2** » presente all'interno della cartella «**Esercizio_Pratico_U3_W3_L2** » sul Desktop della macchina virtuale dedicata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

DLL MAIN

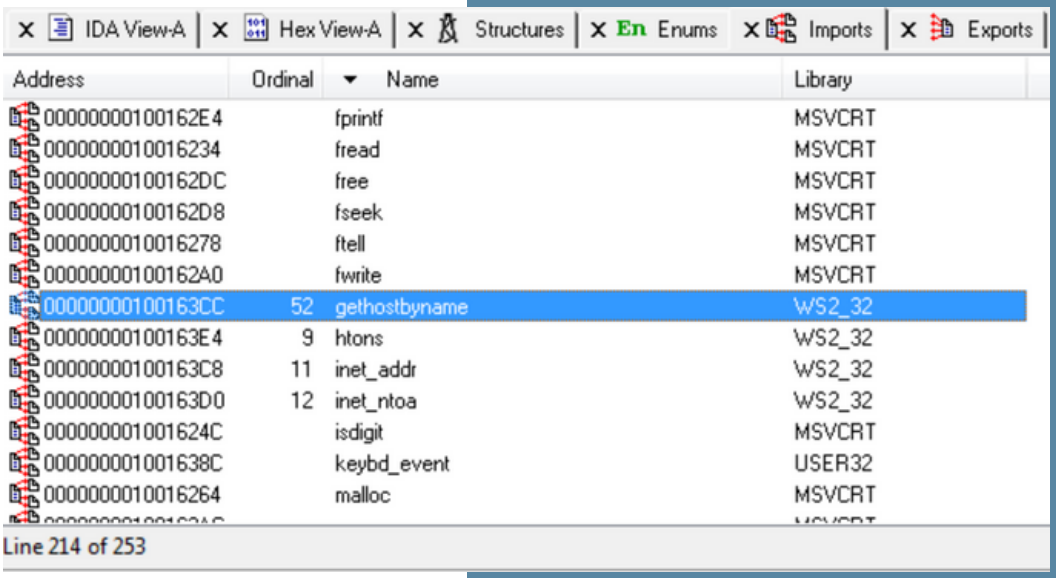


Per recuperare l'entry point basta aprire il nostro Malware tramite l'utilizzo di Ida Pro (Spiegazione accanto), un disassembler già pre installato all'interno della nostra macchina Windows 7. Una volta aperto, passiamo alla modalità testuale per recuperare il Dll Main (1000D02E)

COS'È IDA PRO?

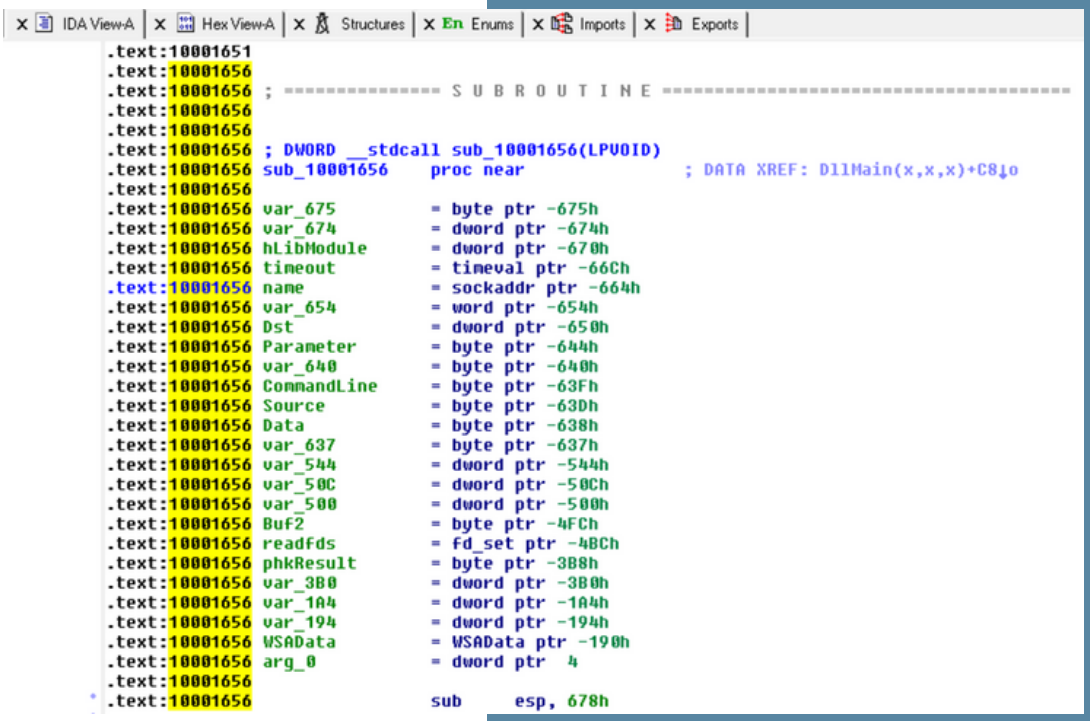
IDA Pro è uno strumento di disassemblaggio e analisi del codice sorgente ampiamente utilizzato nell'ambito della sicurezza informatica e della ricerca sulla sicurezza dei software. Funziona in modo simile a un debugger, ma va oltre nel fornire una vasta gamma di funzionalità per analizzare il codice binario.
IDA Pro analizza il file binario e lo traduce in linguaggio assembly leggibile dall'uomo.

GETHOSTBYNAME



Per scoprire l'indirizzo dell'import gethostbyname basta aprire la finestra degli "imports" su ida pro. come vediamo gethostbyname è all'indirizzo 100163cc, come vediamo in figura.

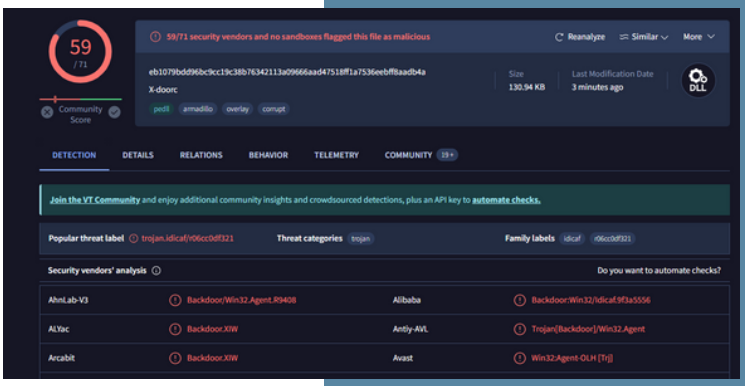
VARIABILI LOCALI



le variabili locali della funzione alla locazione di memoria 10001656 sono in totale 20 (qui nella foto se ne vedono 33, ma sappiamo che le variabili vengono considerate locali quando hanno offset negativo rispetto all'ebp).
Per quanto riguarda invece i parametri trovati, notiamo un solo argomento con offset positivo rispetto all' EBP. IDA ha chiamato questo parametro arg_0.

ASSEMBLY

COMPORTAMENTO DEL MALWARE



Il compito coinvolge l'esecuzione di un file DLL malevolo utilizzando il processo Windows legittimo "rundll32.exe" da una cartella temporanea nella directory del profilo utente. Il processo genitore per questa esecuzione è stato identificato come un processo con PID 1164.

Uno dei punti più interessanti in questo compito è l'uso del processo rundll32.exe per caricare ed eseguire il file DLL malevolo. Questa tecnica è comunemente utilizzata dai malware per evitare la rilevazione poiché rundll32.exe è un processo Windows legittimo. Inoltre, il fatto che il file DLL fosse situato nella cartella temporanea dell'utente indica un tentativo di mimetizzarsi con l'attività utente normale e evitare la rilevazione.

In conclusione, il compito coinvolgeva l'esecuzione di un file DLL potenzialmente malevolo utilizzando un processo Windows legittimo, indicando un possibile tentativo di evitare la rilevazione. Gli analisti di malware dovrebbero prestare particolare attenzione a tali tecniche che coinvolgono l'albero dei processi e posizioni di file sospette per identificare ed attenuare efficacemente le potenziali minacce.

GRAZIE

PHANTOM SRL

PREPARED BY

PIGNATELLO GIUSEPPE
D'OTTAVIO ALESSIO
IANNONE LUCA