Pratica S11/L3

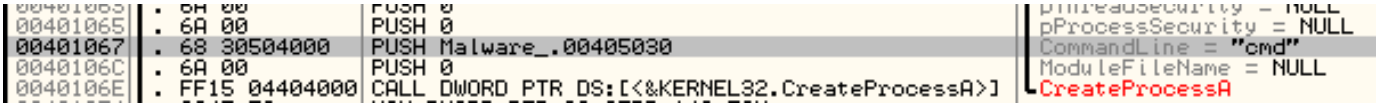
Traccia:
Fate riferimento al malware: Malware_U3_W3_L3, presente all'interno della cartella Esercizio_Pratico_U3_W3_L3sul desktop della macchina virtuale dedicata all'analisi dei malware.
Rispondete ai seguenti quesiti utilizzando OllyDBG.

- All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (**1**)
- Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (**2**) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (**3**) motivando la risposta (**4**). Che istruzione è stata eseguita? (**5**)
- Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (**6**) Eseguite un step-into. Qual è ora il valore di ECX? (**7**). Spiegate quale istruzione è stata eseguita (**8**).

Bonus: Spiegare a grandi linee il funzionamento del malware

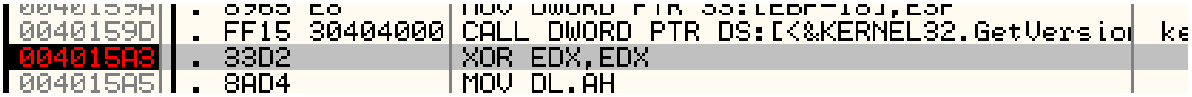
1.Valore del parametro «CommanLine»

Il valore del parametro è «**cmd**», cioè il Prompt dei comandi di Widnows



2.All'indirizzo 004015A3 qual è il valore del registro EDX?

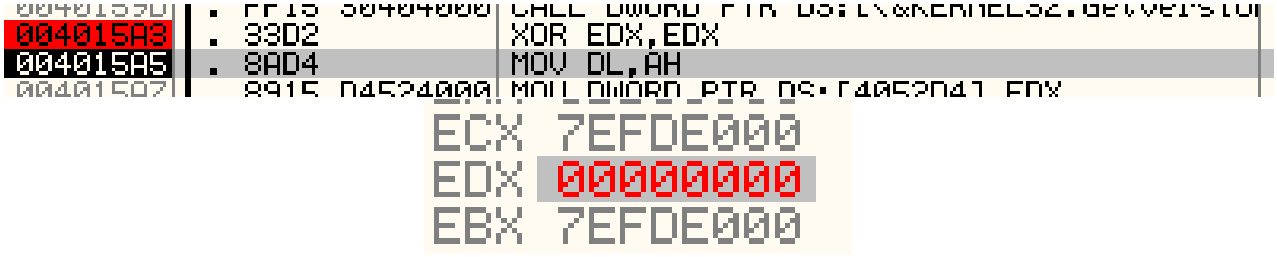
Inserito un breakpoint all'indirizzo **004015A3**



Il valore di EDX è **00001DB1**

3.Eseguire uno «step-into». Qual è ora il valore del registro EDX?

Adesso il valore di EDX è **00000000**



4.Motivare la risposta.

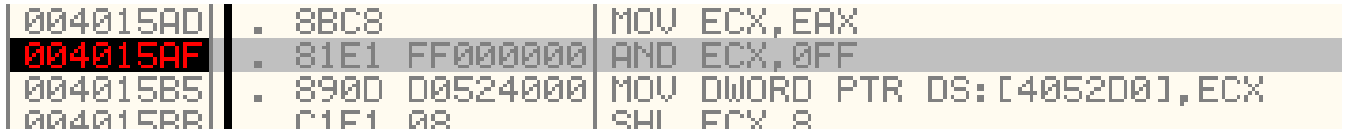
Dopo aver inserito il breakpoint all'indirizzo **004015A3**, cliccando su Play il programma si ferma sull'istruzione **XOR EDX, EDX** indicado il valore di **EDX**.

5.Che istruzione è stata eseguita?

Dopo lo «**step-into**» viene eseguito **XOR EDX, EDX** azzerando il valore di EDX portandolo a **0**

6.All'indirizzo 004015AF qual è il valore del registro ECX?

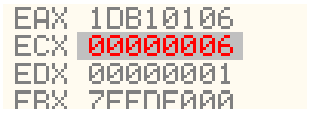
Inserito un breakpoint all'indirizzo **004015AF**



Il valore di ECX è **0DB10106**

7.Eseguire uno «step-into». Qual è ora il valore di ECX?

Adesso il valore è **00000006**



8.Spiegare quale istruzione è stata eseguita.

L'istruzione eseguita è **AND ECX, 0FF**

Bonus: Spiegare a grandi linee il funzionamento del malware

Il file Malware_U3_W3_L3 è un Trojan Horse (info Virus Total).
Utilizzare il Prompt dei Comandi di Windows per poter creare un file all'interno del disco in modo, anche in un secondo momento, per prenderne il controllo.