Esercizio S11/L3

Malware analysis dinamica con Ollydbg

Traccia

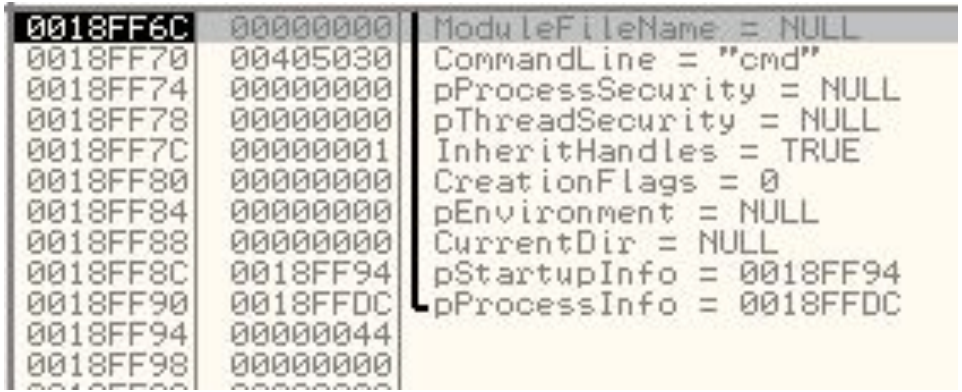
Fate riferimento al malware: **Malware_U3_W3_L3**, presente all'interno della cartella **Esercizio_Pratico_U3_W3_L3** sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

- 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

Punto 1

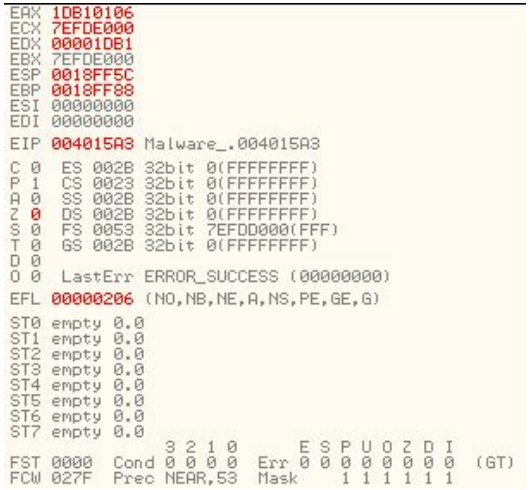
Ollydbg (Olly debug) è un software per windows in grado di analizzare un eseguibile mentre è in esecuzione. In tempo reale riesce a tracciare i registri, identificare le funzioni con i parametri e le variabili che vengono passate sullo stack.

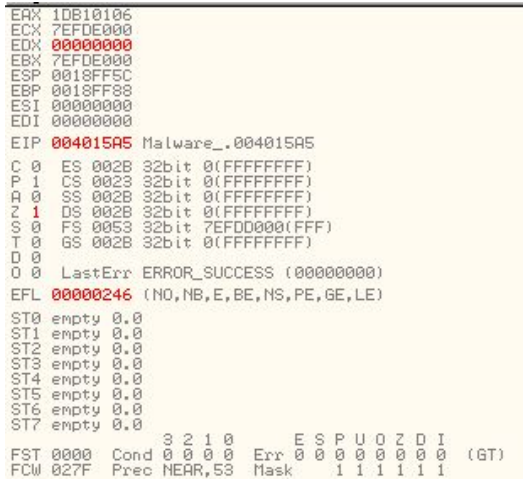
Nella figura accanto possiamo vedere la finestra di ollydbg che mostra lo stack di memoria. Il parametro della “Commandline” passato sullo stack è “cmd”, cioè la shell di windows.



Punti 2, 3, 4 e 5

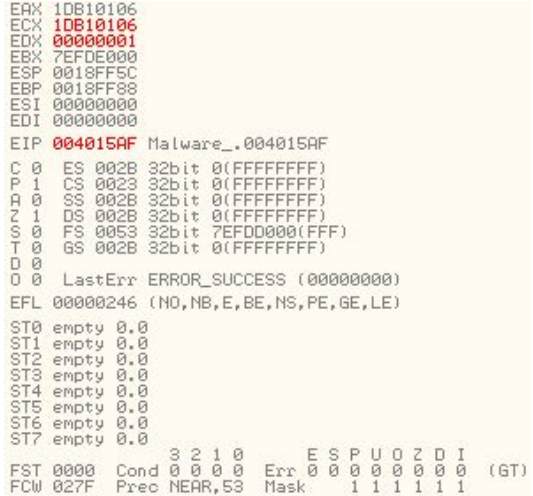
All’indirizzo 004015A3, come vediamo dalla prima figura, inizialmente il valore del registro EDX è 1DB1 (7601 convertito in decimale). Nella seconda figura il valore diventa 0, dopo aver effettuato lo step-into. Questo perchè viene eseguito lo XOR del registro EDX con se stesso, che da come risultato sempre 0.

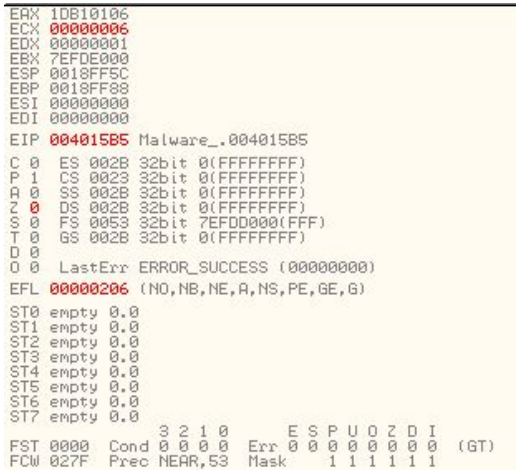




Punti 6, 7 e 8

All’istruzione 004015AF inizialmente il valore di ECX è 1DB10106 (498139398 convertito in decimale) e poi, dopo lo step-into, diventa 6. L’istruzione che viene eseguita è l’AND, cioè il prodotto logico.





Bonus

Data la presenza di una istruzione che cerca di aprire una shell (Commandline) possiamo ipotizzare che il malware in questione sia un rootkit.