S11/L3

TRACCIA

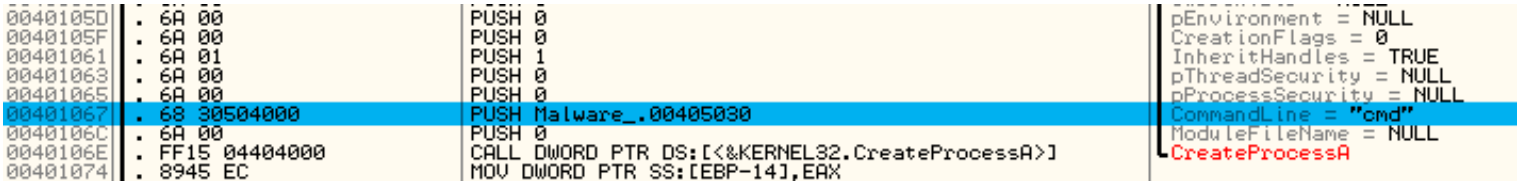
Analizzare il malware **Malware_U3_W3_L3** rispondere ai seguenti quesiti utilizzando OllyDBG:

1. 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?
2. Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?
3. Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? Eseguite un step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.
4. BONUS: spiegare a grandi linee il funzionamento del malware

ESERCIZIO

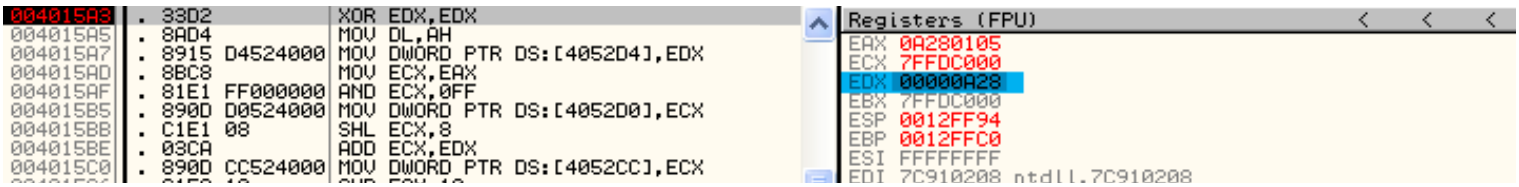
1.

Analizzando l'indirizzo di memoria **0040106E** possiamo notare che il valore della funzione è **cmd** come evidenziato in figura.
CMD è il Prompt dei Comandi disponibile nella maggior parte dei sistemi operativi Windows, che viene utilizzato per eseguire dei comandi immessi dall'utente.

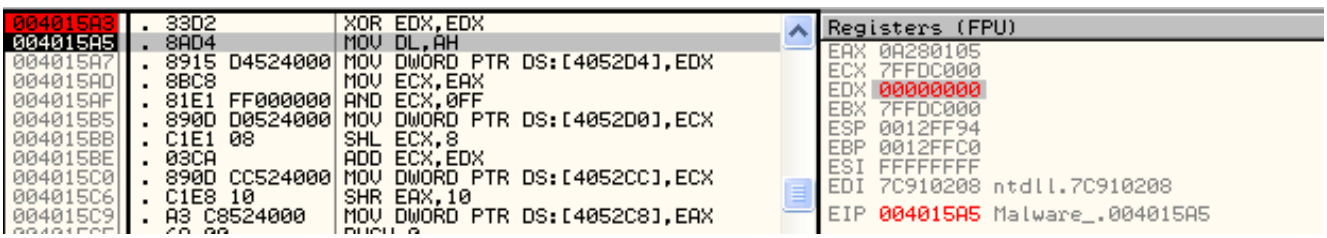


2.

Andando ad inserire un breakpoint software attraverso il comando "Toggle Breakpoint" sull'indirizzo di memoria **004015A3** possiamo fermare il programma in esecuzione per analizzare più nello specifico il malware senza che il debugger continui a leggerlo. Una volta fatto ciò, possiamo vedere che il valore di EDX corrisponde a **00000A28**

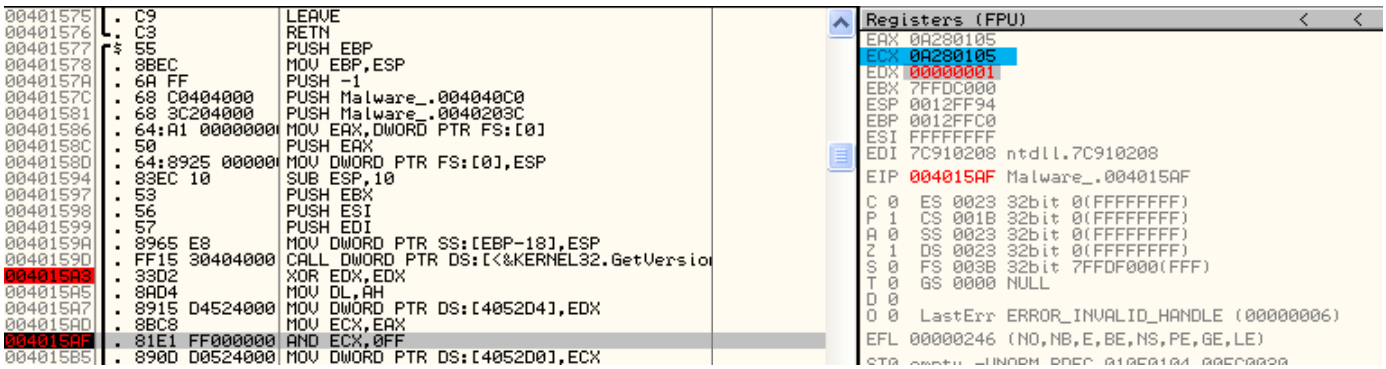


Con la funzione "step-into" andremo ad analizzare la funzione dove viene implementata. Nel nostro caso possiamo notare che il registro EDX è inizializzato a zero come riportato dallo XOR individuato nella chiamata di funzione.

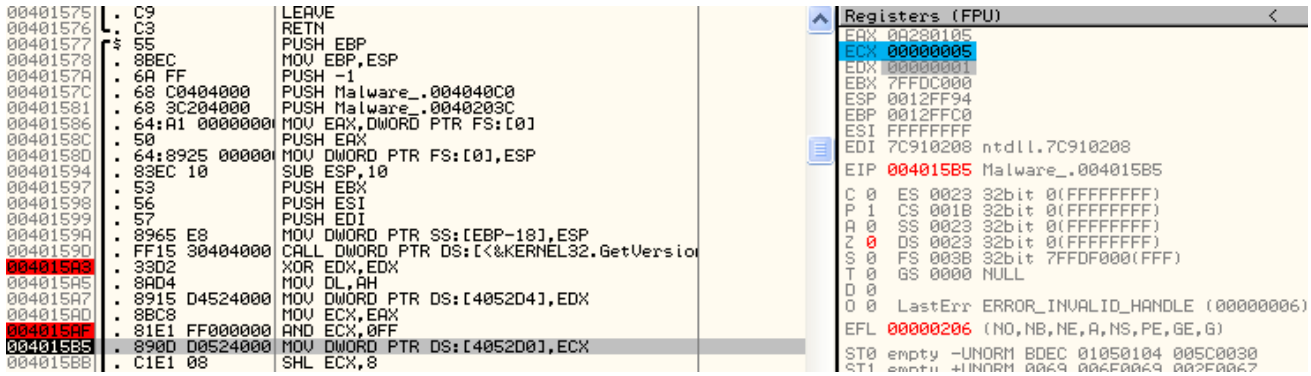


3.

Ripetendo lo stesso procedimento come nel punto **2** inseriremo un breakpoint software sull'indirizzo di memoria **004015AF**. Possiamo vedere come in figura che il valore di ECX corrisponde a **0A280105**.



Eseguendo uno "step-into" possiamo vedere che il valore di EXC cambia in **00000005**



In questo caso viene eseguita l'istruzione AND sui bit ECX ed il valore 0FF (in esadecimale 255).