Malware analysis OllyDbg

Richiesta: 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.

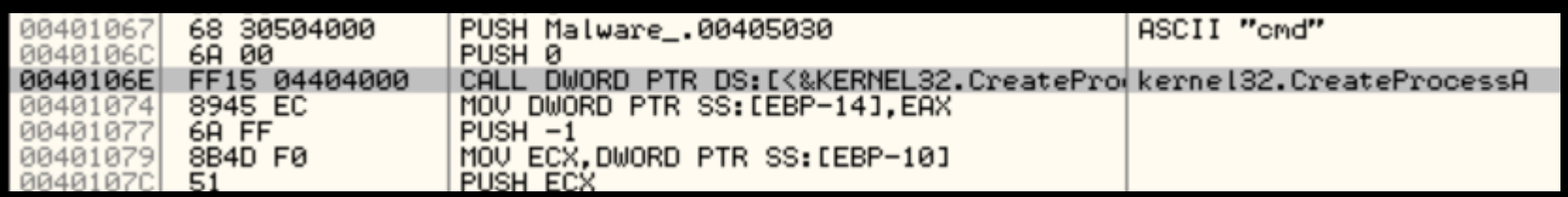
Rispondeyìte ai seguenti quesiti utilizzando OllyDBG:

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?
3. Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX, motiva 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

BONUS: spiegare a grandi linee il funzionamento del malware

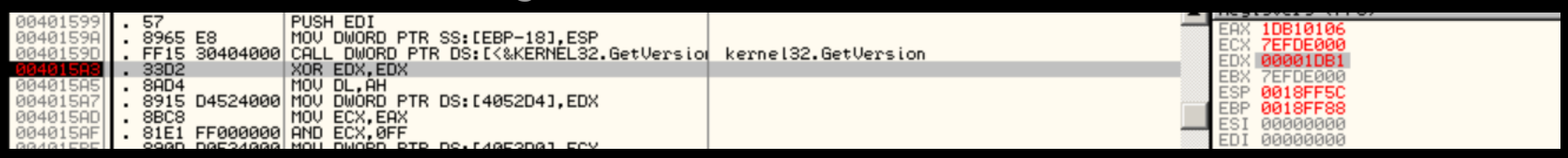
Valore del parametro CommandLine

Il valore del parametro CommandLine che viene passato sullo stack è “CMD”, rappresenta il command prompt di Windows, osservabile all’indirizzo 0040167.



Breakpoint indirizzo 0040153A3

Configuriamo il breakpoint all’indirizzo in questione, avviamo il programma e osserviamo il valore del registro EDX una volta fermatosi



Il valore del registro EDX è 00001DB1

Step-into

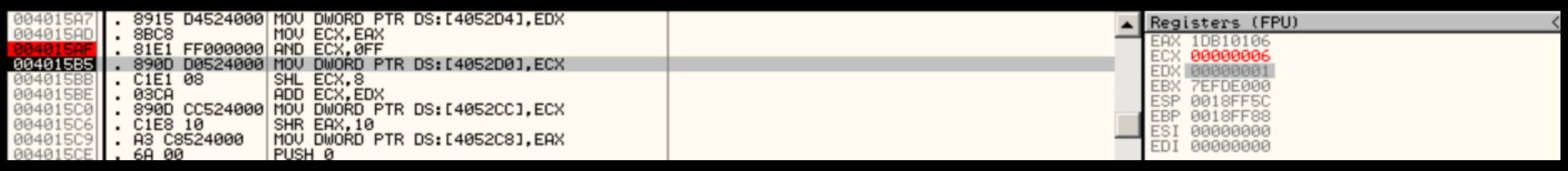
Adesso eseguiamo lo step-into, che eseguirà l'istruzione XOR EDX, EDX, che serve ad azzerare il contenuto del registro EDX.

Il valore del registro EDX è 00000000

Breakpoint indirizzo 004015AF

Configuriamo un secondo breakpoint all'indirizzo selezionato, il valore del registro ECX è 1DB1016

Adesso eseguiamo lo step-into, notiamo che il valore del registro ECX è 00000006 dopo aver eseguito l'istruzione AND ECX, 0FF



Qui l'istruzione esegue l'AND sui bit di ECX e del valore di FF (esadecimale), dando come risultato il valore di ECX ottenuto dopo lo step-into.