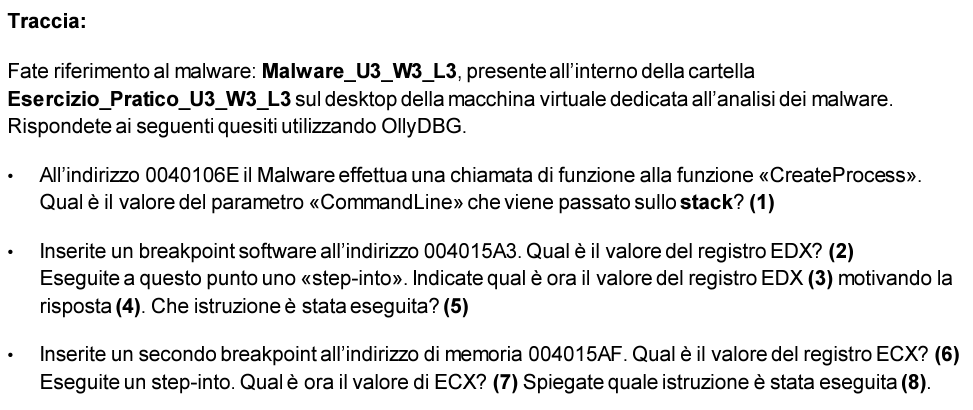
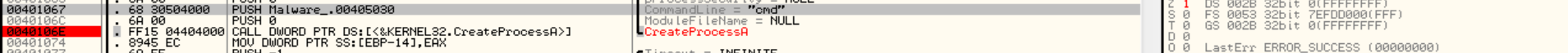
Analisi malware avanzata tramite OllyDBG

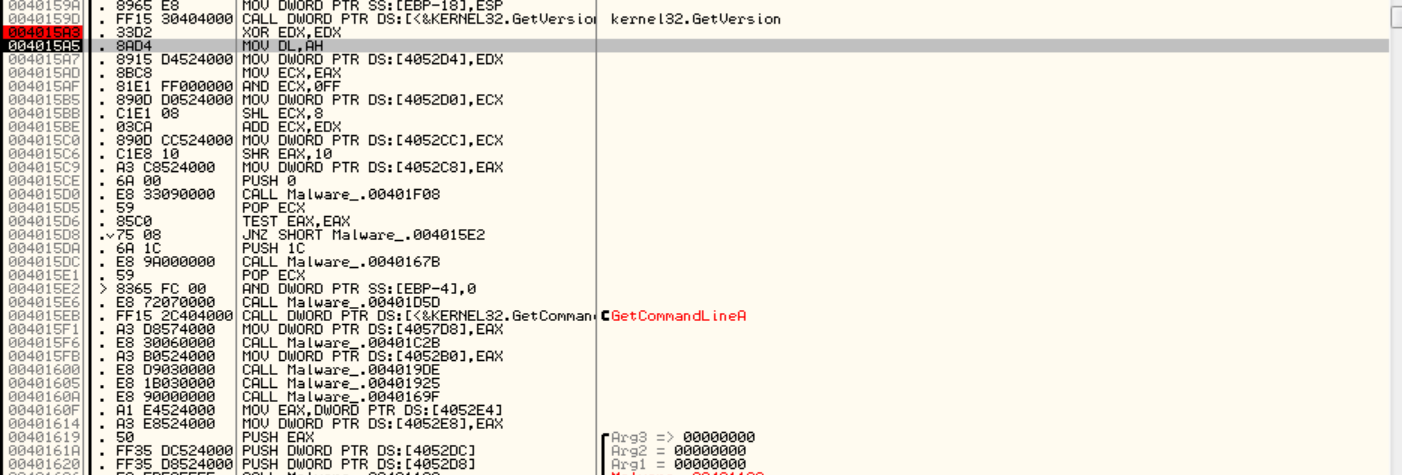


1) All’indirizzo 0040106E il Malware effettua una chiamata di funzione ”CreateProcess”. Qual è il valore del parametro “CommandLine” che viene passato sullo stack?



Il valore del parametro “CommandLine” che viene passato sullo stack è “cmd”, ovvero il command prompt di Windows, presente all’indirizzo 00401067

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?



Una volta che avremo configurato il brakpoint, possiamo avviare il malware il quale si fermerà all’istruzione XOR EDX, EDX. Prima dell’esecuzione il valore del regitro è 00000A28, successivamente, a seguito dello step-into, l’istruzione XOR EDX, EDX verrà eseguita andando così a inizializzare a zero una variabile.

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.



Una volta inserito il brakpoint all’indirizzo 004015AF, avviato ed eseguito lo step-into, il registro ECX avrà un valore modificato a 00000005 in quanto sarà stata eseguita l’istruzione AND ECX, FF.

Più precisamente l’istruzione andrà ad eseguire l’AND logico sul registro EAX e sul valore esadecimale FF. Quindi per eseguire il calcolo convertiamo i valori in decimale e poi si eseguirà l’AND logico sui bit.



A seguito dell'esecuzione dell’AND logico sui bit otteniamo:

0000 0000 0000 0000 0000 0000 0000 0101

il quale in esadecimale sarà 00000005, andando così a spiegare listruzione AND ECX, OFF.