PRATICA S11_L3

OllyDBG

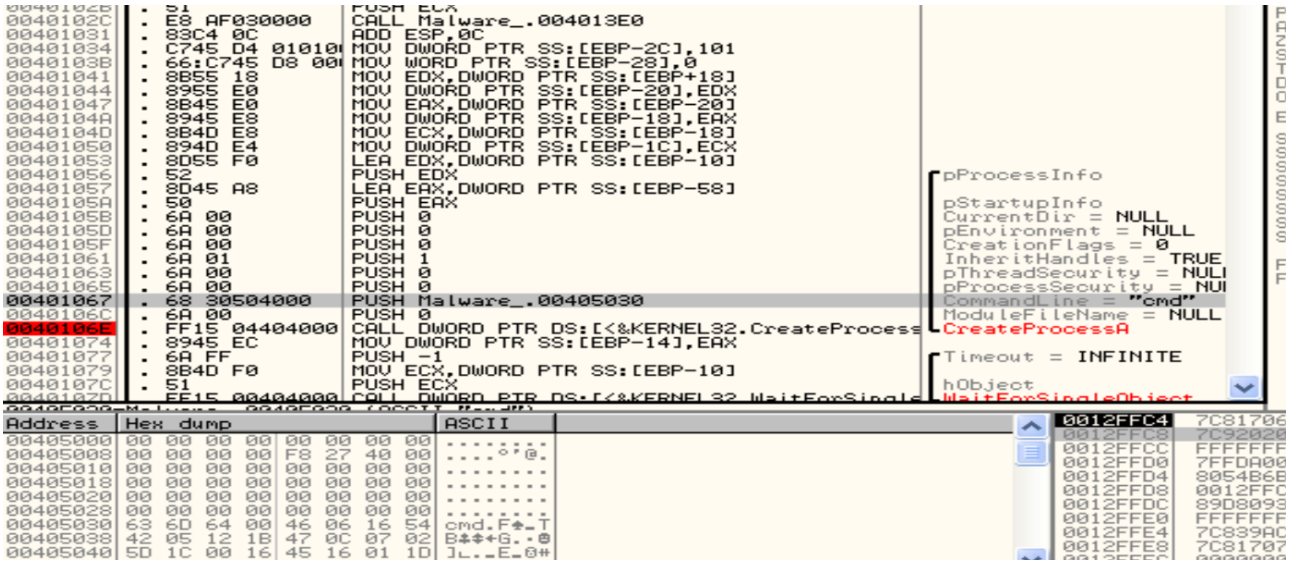
Con riferimento al malware “Malware_U3_W3_L3” presente all’interno della cartella “Esercizio_Pratico_U3_W3_L3” sul desktop della macchina virtuale Windows XP dedicata all’analisi dei malware, rispondere ai seguenti quesiti utilizzando OllyDBG:

- **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» e 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 poi uno step-into, qual’è ora il valore di ECX? Spiegate quale istruzione è stata eseguita

SOLUZIONI:

Dopo aver preparato la macchina virtuale, disattivando le connessioni esterne ad internet ed ogni instradamento pericoloso verso la macchina host e dispositivi di archiviazione esterni, procedo con le soluzioni:

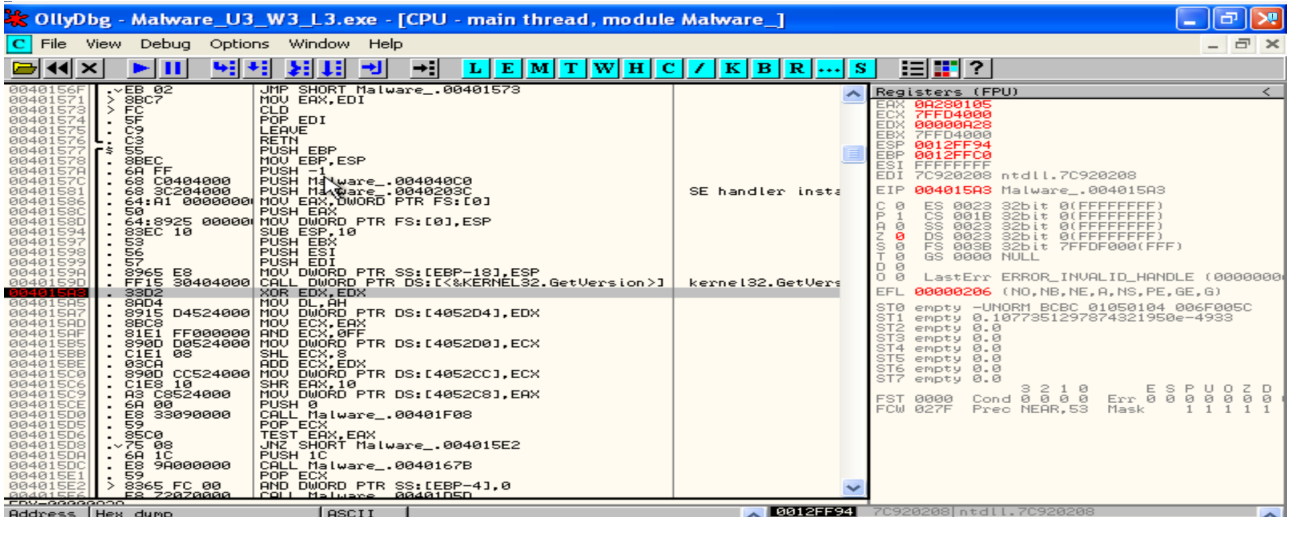
1)



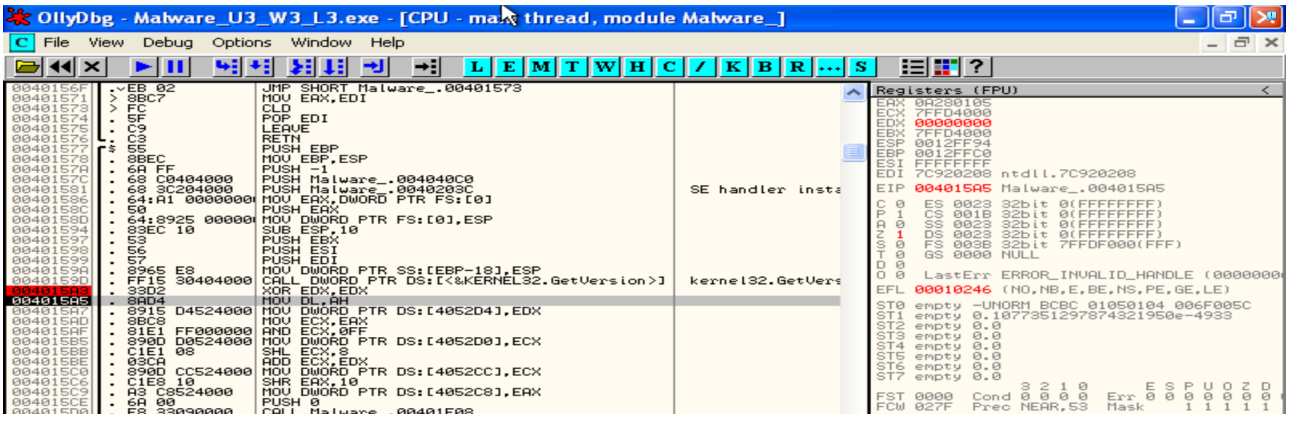
All’indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess», il valore del parametro «CommandLine» che viene passato sullo stack è “cmd” ovvero il comando per avviare il command prompt di Windows.

2)

PRIMA



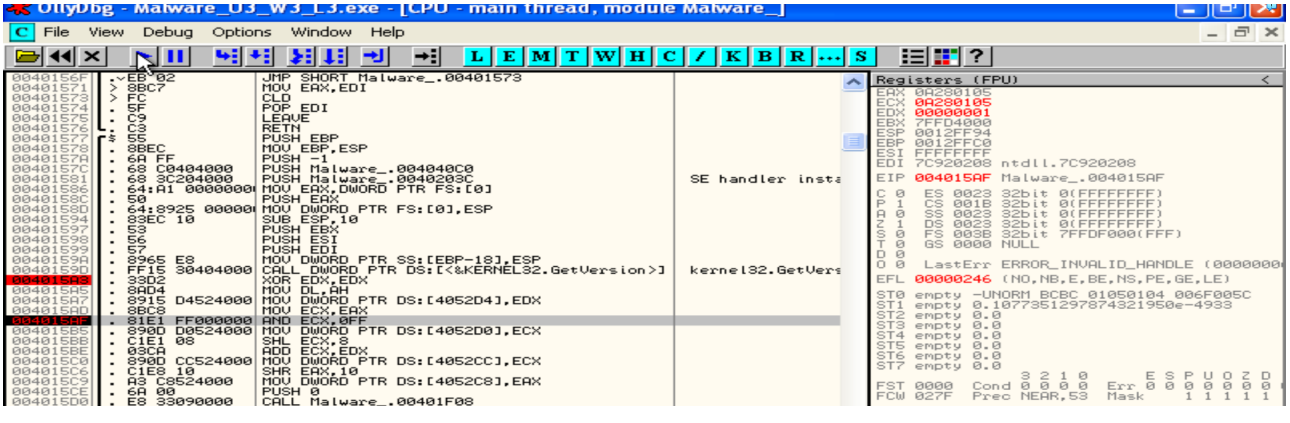
DOPO



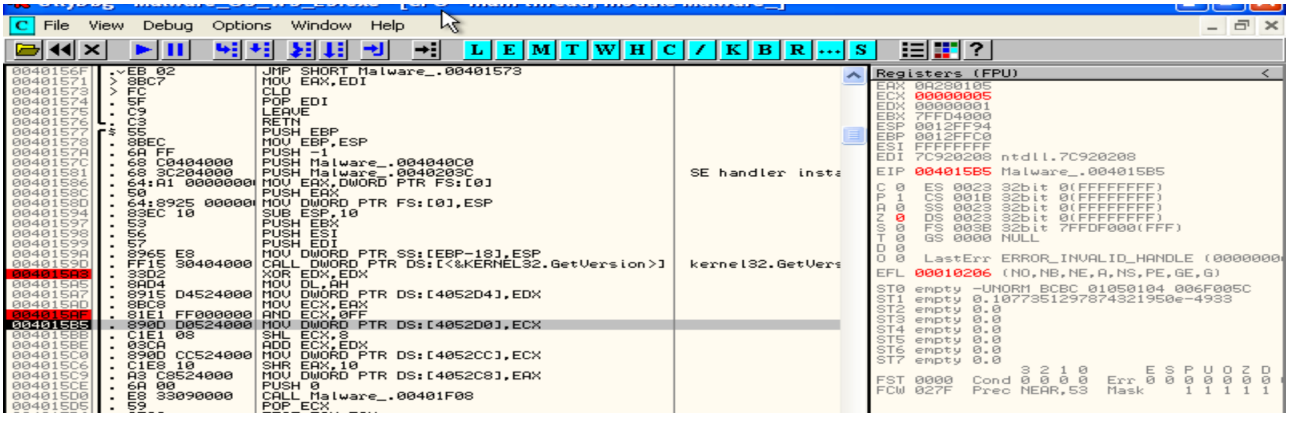
Inserito il breakpoint software all'indirizzo 004015A3, il valore del registro EDX è "00000A28". Eseguito uno «step-into», il valore del registro EDX diventa "00000000" poiché lo "XOR EDX, EDX" dello stesso registro (cioè con se stesso) inizializza a zero il suo valore, essendo che l'operazione XOR (exclusive OR) tra due bit restituisce 1 se i bit sono diversi e 0 se i bit sono uguali.

3)

PRIMA



DOPO



Inserito un secondo breakpoint all’indirizzo di memoria 004015AF, il valore del registro ECX è “0A280105”. Eseguito poi uno step-into, il valore di ECX diventa “00000005”,perchè è’ stata eseguita l’istruzione “AND ECX, 0xFF” che esegue un'operazione logica di AND bit a bit tra il registro ECX e il valore immediato 0xFF. L'operatore AND restituisce 1 solo se entrambi i bit corrispondenti sono 1, altrimenti restituisce 0. Quindi traducendo il valore esadecimale di ECX e di 0xFF in bit, ed operando l’AND tra i bit di entrambi, si ottiene appunto il valore di 00000005.