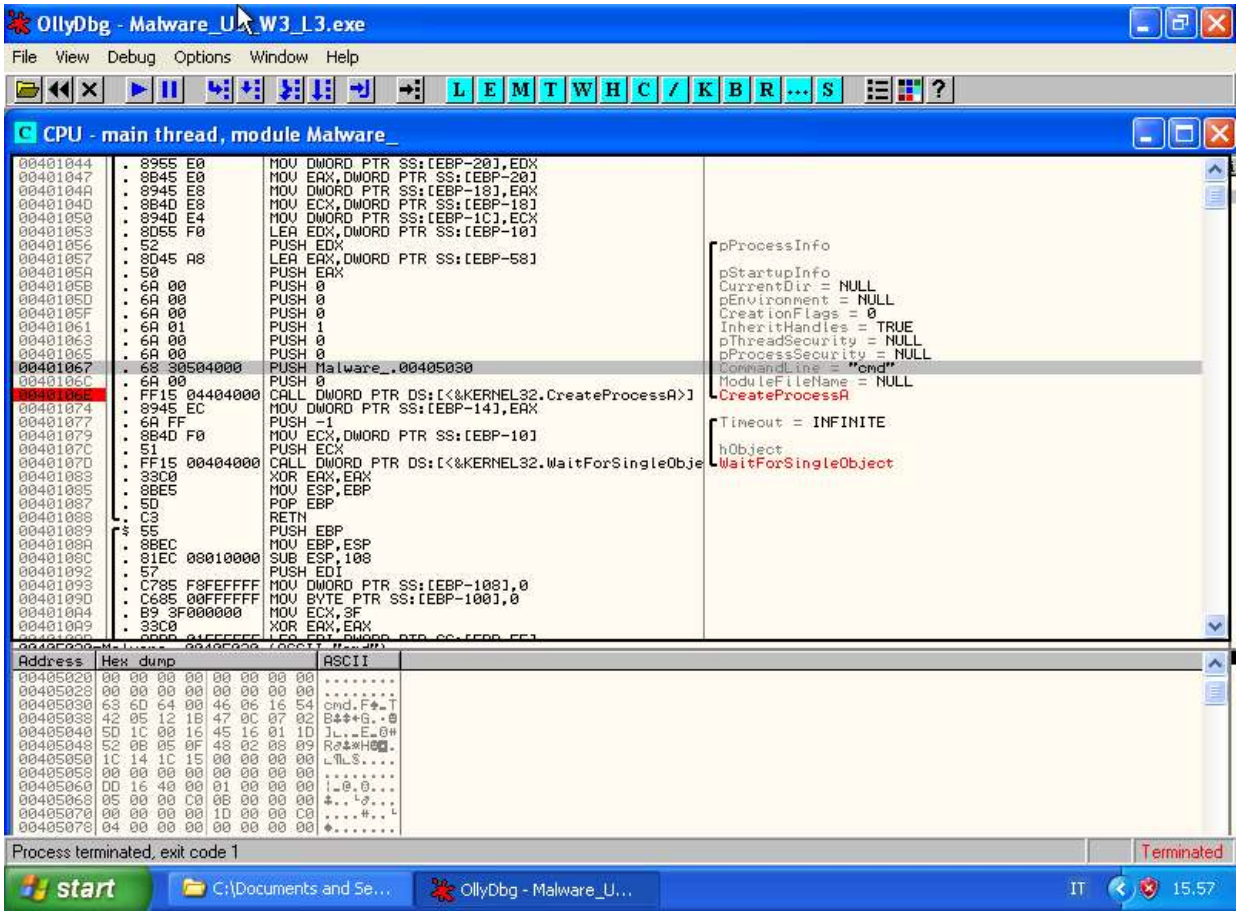
Esercizio Epicode 12/07/2023

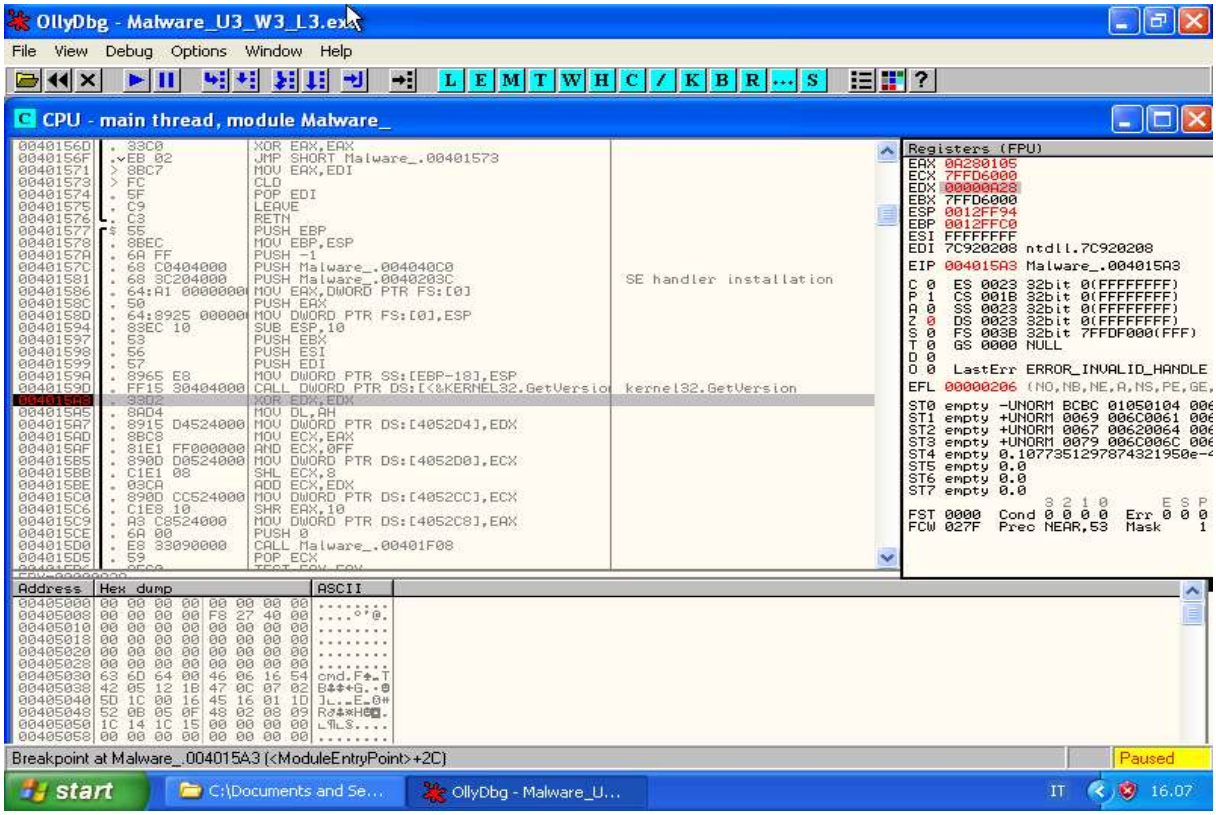
Punto 1:

il valore del parametro **CommandLine** è **cmd** ovvero avvia il prompt dei comandi.

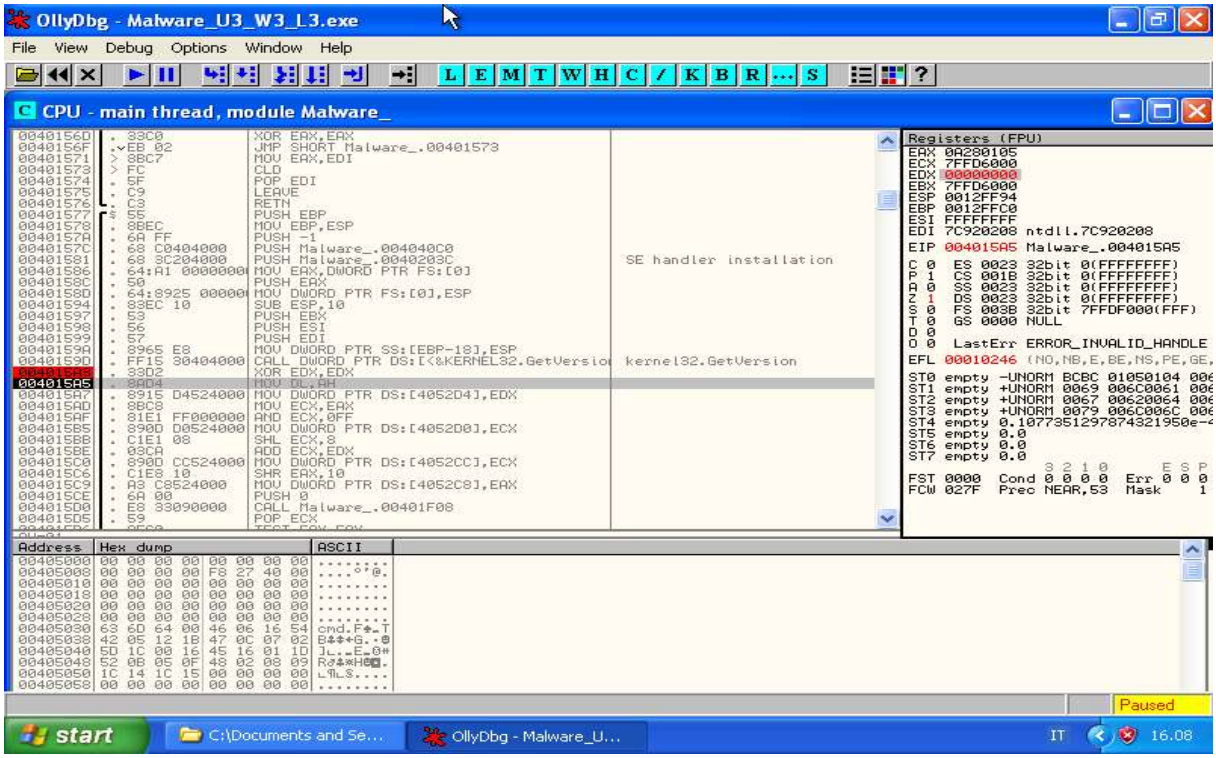


Punto 2:

Dopo aver inserito un breakpoint all'indirizzo di consegna, posso constatare che il valore del registro EDX è **00000A28**



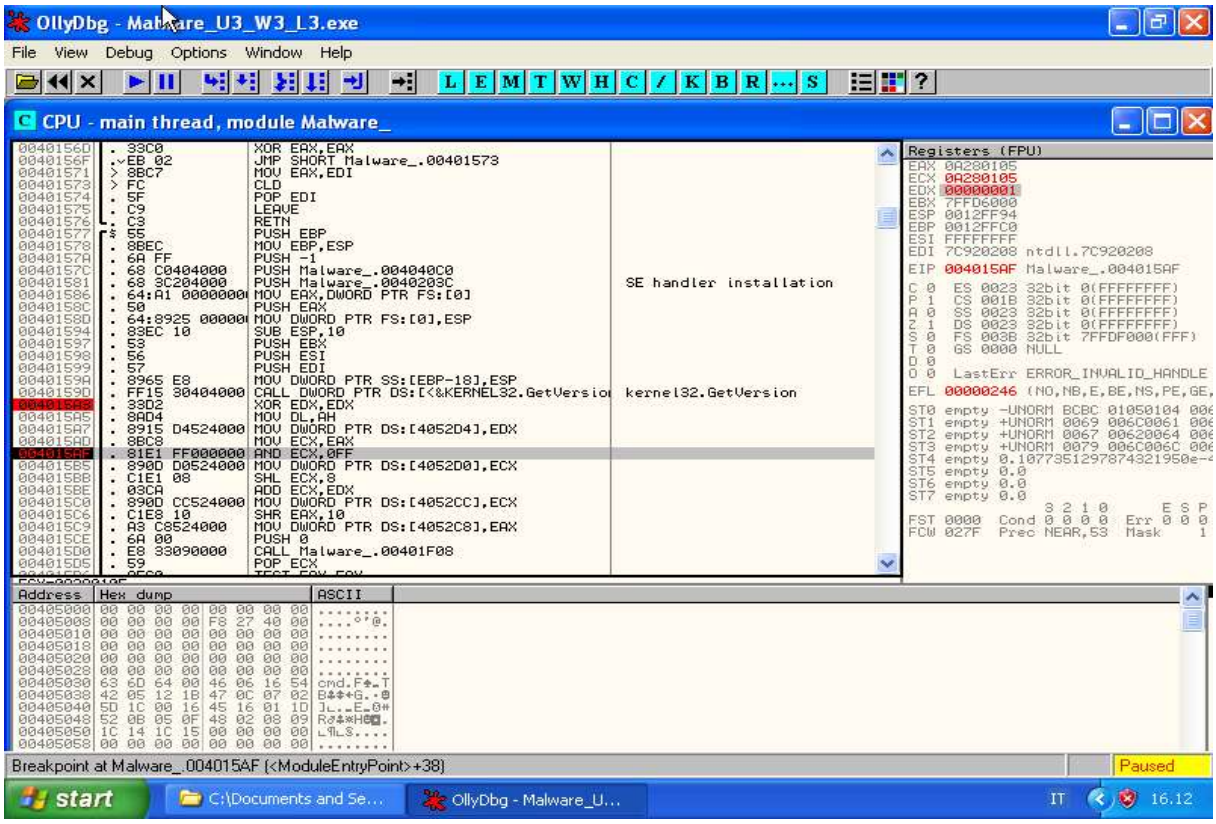
Dopo aver seguito uno **step into**, noto il cambiamento del valore del registro EDX in 00000000



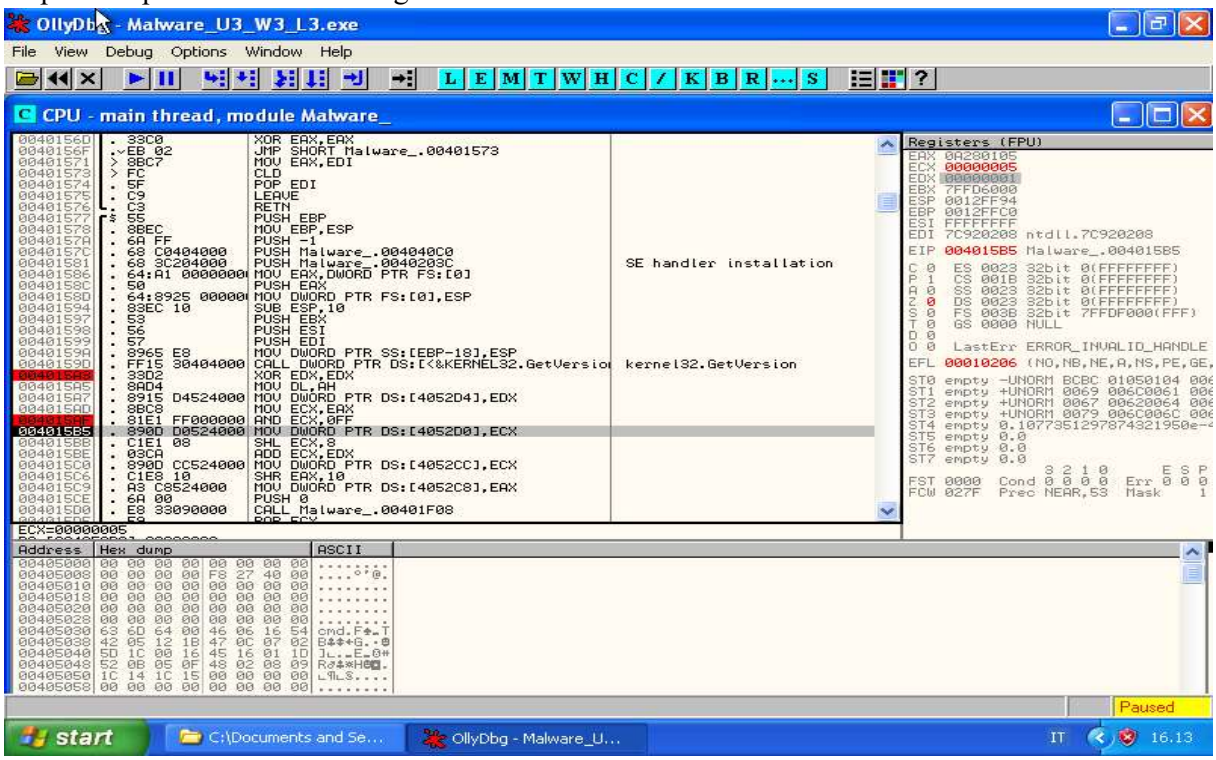
Essendo stata eseguita un'istruzione XOR con x = y il risultato è 0

Punto 3:

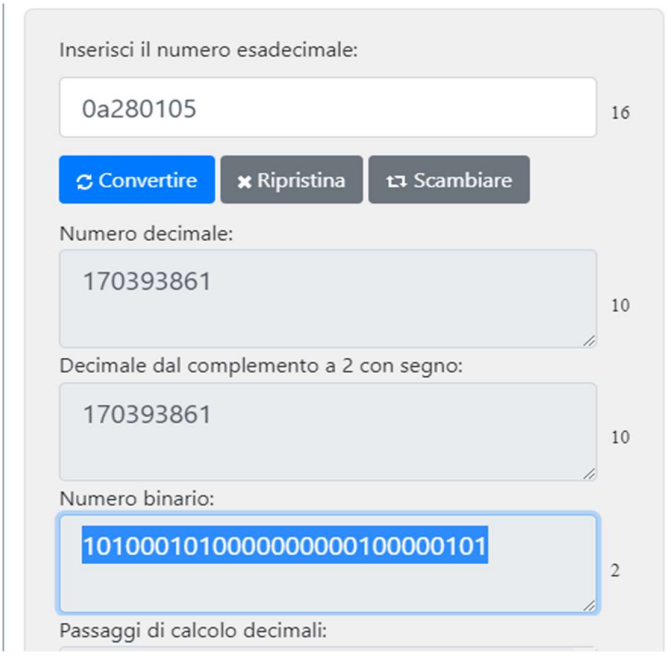
Ho inserito un secondo breakpoint all'indirizzo come da consegna. Il valore del registro ECX è 0A280105.

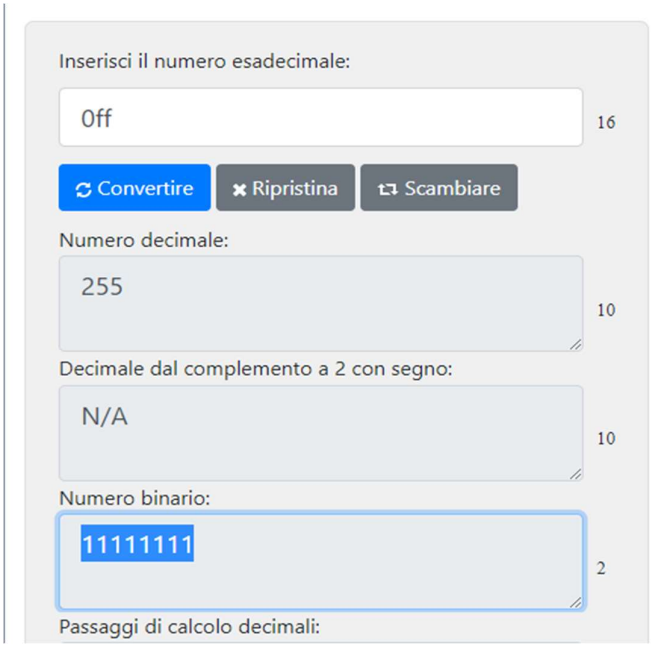


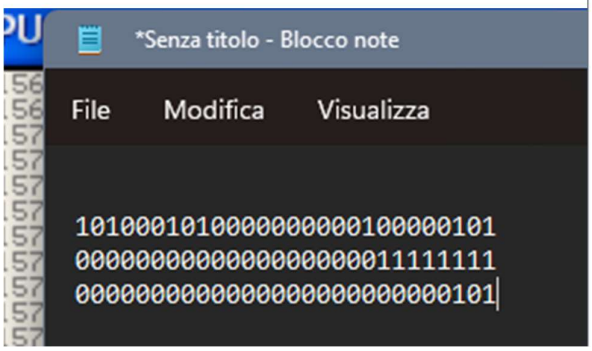
Dopo lo step into il valore del registro ECX è cambiato in 00000005.

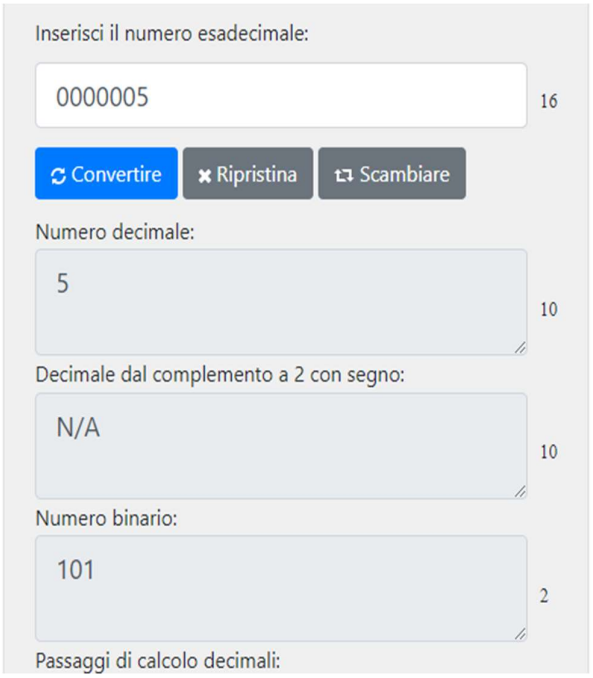


È stata eseguita un'istruzione AND, per verificarne la correttezza ho convertito in binario il valore esadecimale del valore del registro ECX e il valore 0FF, ed effettuato il calcolo dell'AND, dopodichè ho convertito il valore binario in esadecimale.









Bonus:

Sembra che il malware sia una backdoor ovvero tenti di aprire una shell cmd per iniettare codice malevole, inoltre cerca di creare un socket per l'invio e ricezione di dati in un dato host.

La funzione WSASocket crea un socket associato a un provider di servizi di trasporto specifico.

La funzione gethostbyname recupera le informazioni sull'host corrispondenti a un nome host da un database host.