S11 L3

Report Esercizio Malware Analysis

GiuliaSalani

INDICE

TRACCIA

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. Rispondete ai seguenti quesiti utilizzando OllyDBG.

- 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? (1)

- Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (2) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3) motivando 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 uno step-into. Qual è ora il valore di ECX? (7) Spiegate quale istruzione è stata eseguita (8).

- BONUS: spiegare a grandi linee il funzionamento del malware

SVOLGIMENTO

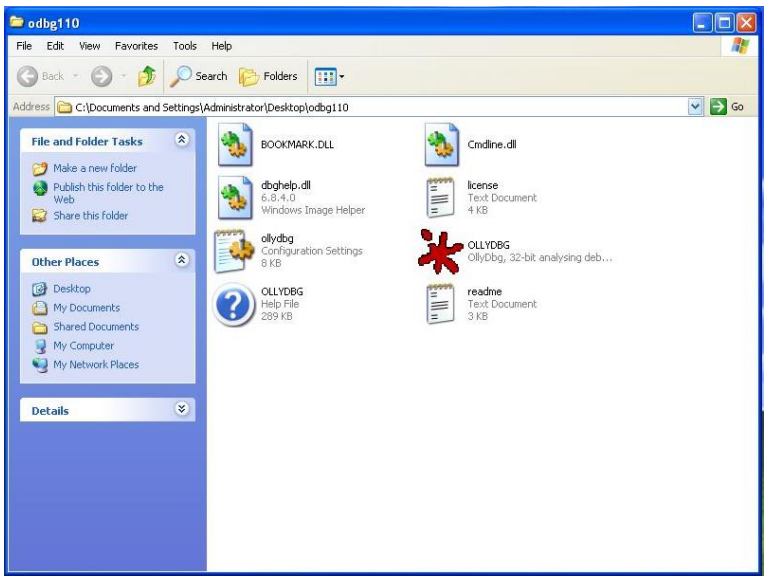
DEFINIZIONE: OLLY DBG

OllyDbg è un **debugger per analisi e reverse engineering di software**. Si tratta di un'applicazione software utilizzata principalmente nel campo della sicurezza informatica e dello sviluppo software. OllyDbg consente agli sviluppatori e agli esperti di sicurezza di esaminare il codice eseguibile di un programma, eseguire il debug in modalità interattiva, analizzare la memoria e monitorare il flusso di esecuzione del programma. Questo strumento è particolarmente apprezzato per la sua interfaccia utente intuitiva e le potenti funzionalità di analisi binaria, rendendolo una risorsa preziosa per la comprensione approfondita del comportamento interno di un'applicazione.

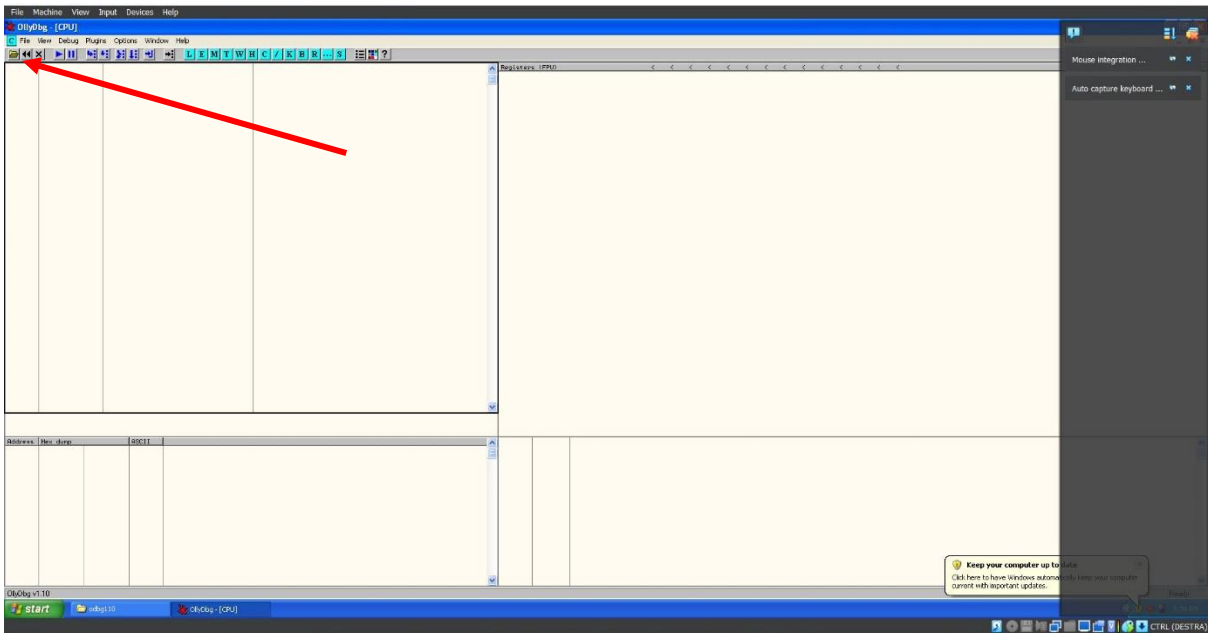
PREPARAZIONE

Come prima cosa, prepariamo il software e carichiamo il malware oggetto dell'analisi odierna. Apriamo la macchina virtuale e individuiamo la cartella che contiene OllyDBG sul desktop:

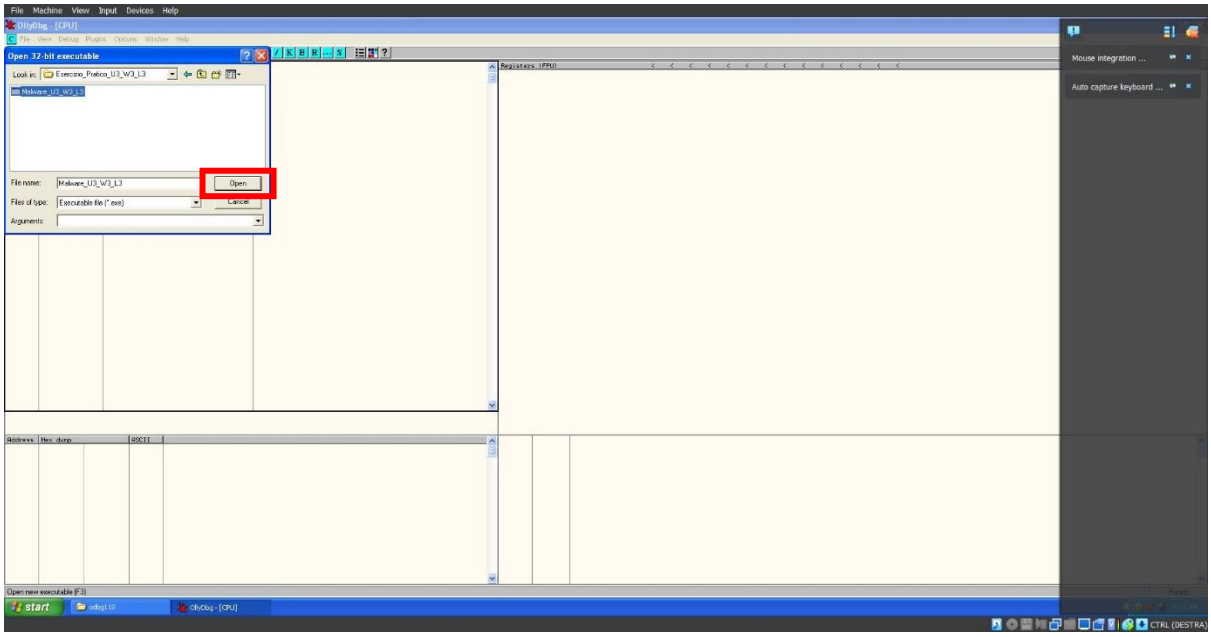
Individuiamo l'eseguibile e con doppio click lo facciamo partire:



Clicchiamo l'icona a forma di cartella in alto a sinistra:



Selezioniamo il file da analizzare e clicchiamo su open:

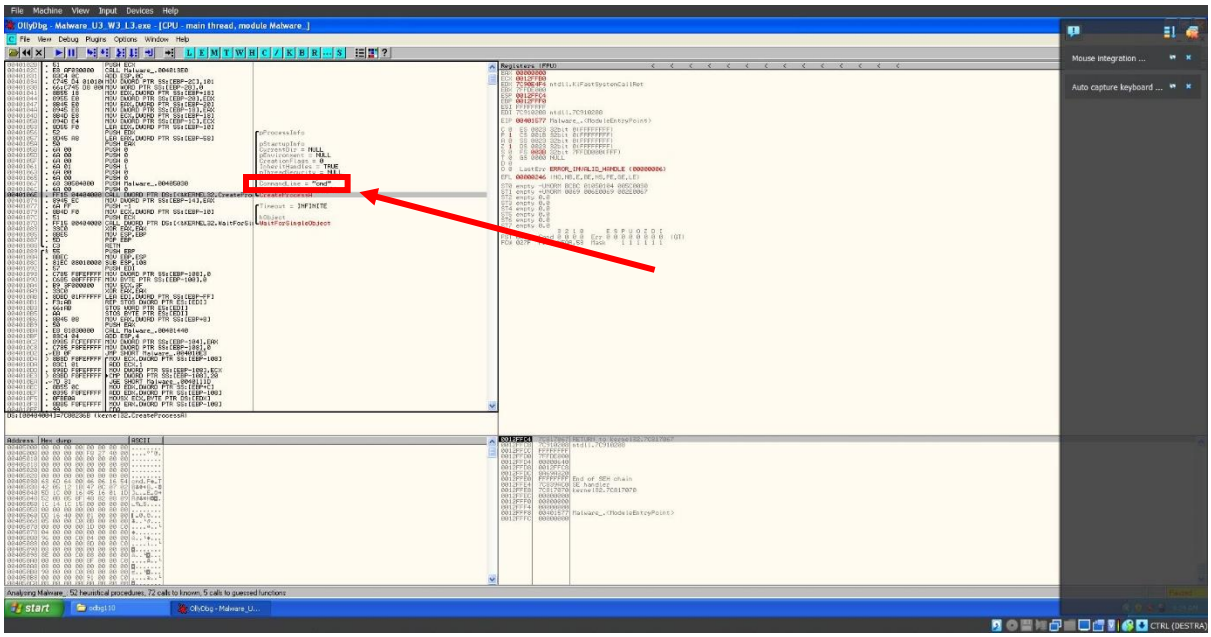


Ora possiamo affrontare le consegne.

QUESITO 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? (1)

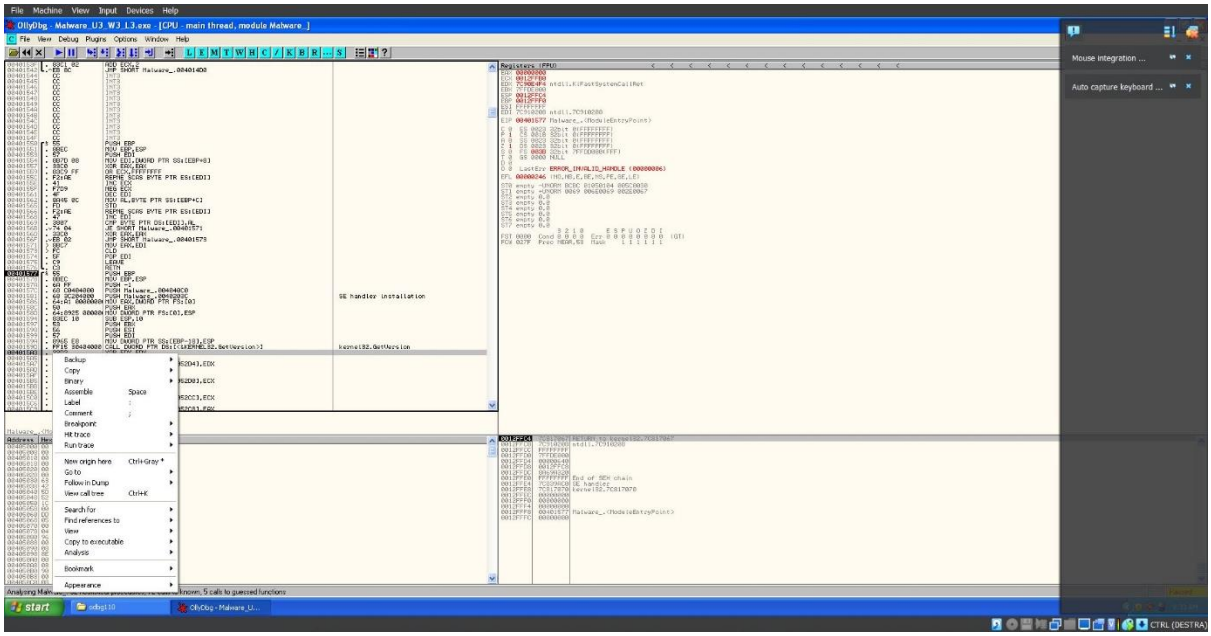
Concentriamoci sul riquadro in alto a sinistra. Scorriamo la lista degli indirizzi di memoria a sinistra fino a incontrare l'indirizzo indicato in consegna. Il parametro di CommandLine è indicato nella quarta colonna e corrisponde a "cmd":



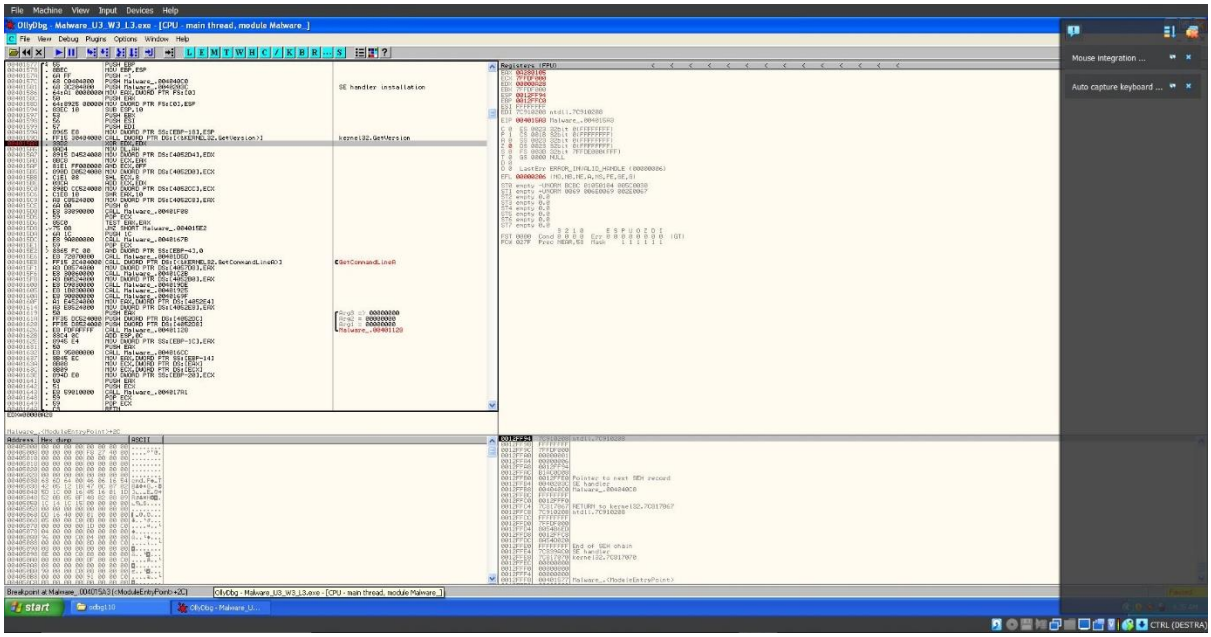
QUESITO 2

Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (2) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3) motivando la risposta (4). Che istruzione è stata eseguita? (5)

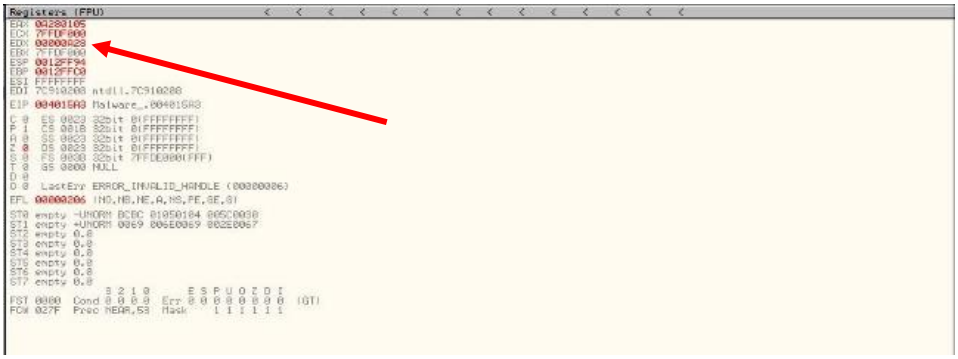
Scorriamo la colonna a sinistra fino a trovare l'indirizzo indicato in questa consegna. Per inserire un breakpoint clicchiamo con il tasto destro sulla riga e alla voce breakpoint selezioniamo il toggle (che sarebbe il software breakpoint):



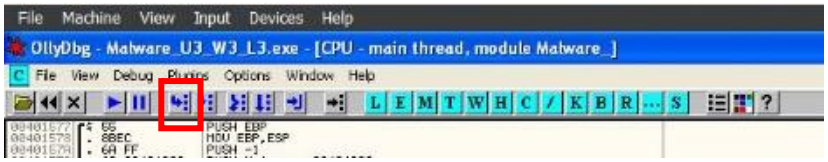
Il valore del registro EDX lo vediamo nel quadrante di fianco a quello utilizzato finora:



Il valore del registro di EDX è 00000A28:



Nella barra in alto selezioniamo questo tasto per effettuare lo step into:



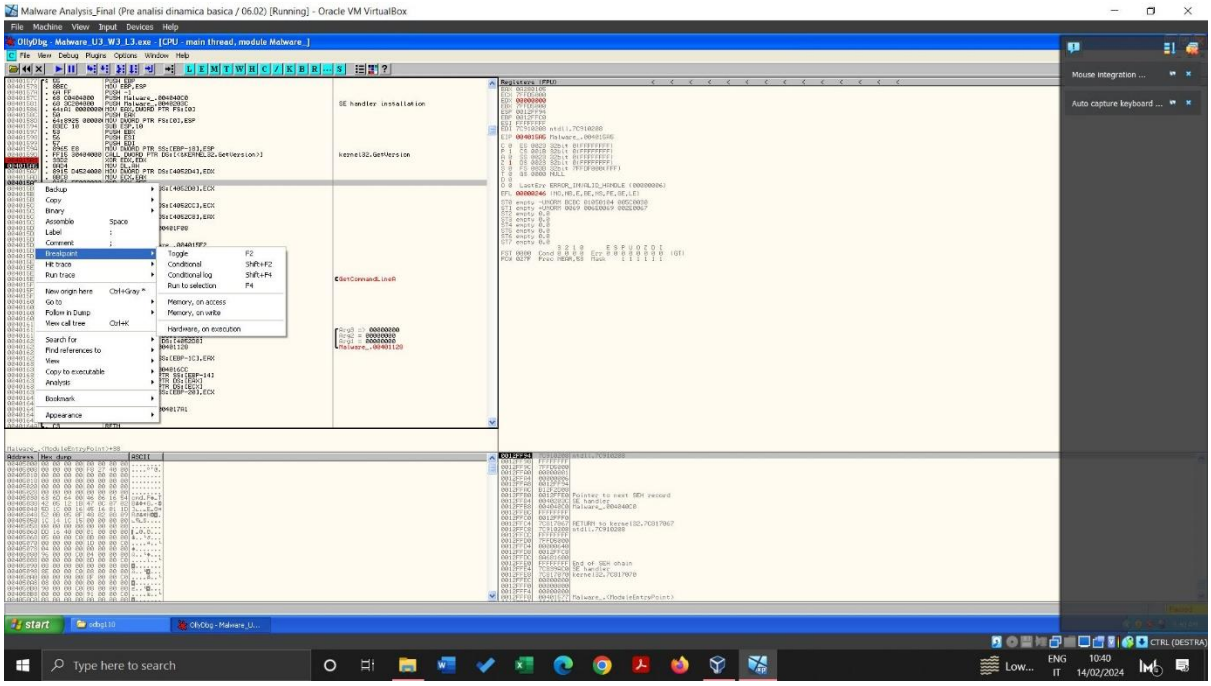
Il nuovo valore di EDX è zero (00000000):

L'istruzione eseguita è stata XOR EDX, EDX il cui scopo è proprio azzerare il registro:

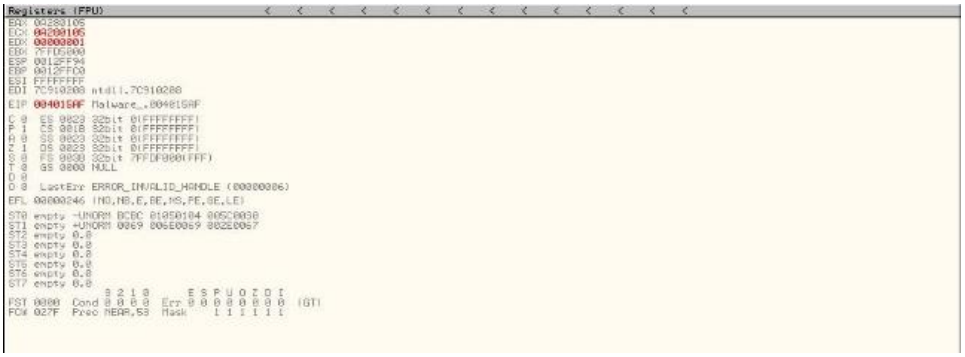
QUESITO 3

Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (6) Eseguite uno step-into. Qual è ora il valore di ECX? (7) Spiegate quale istruzione è stata eseguita (8).

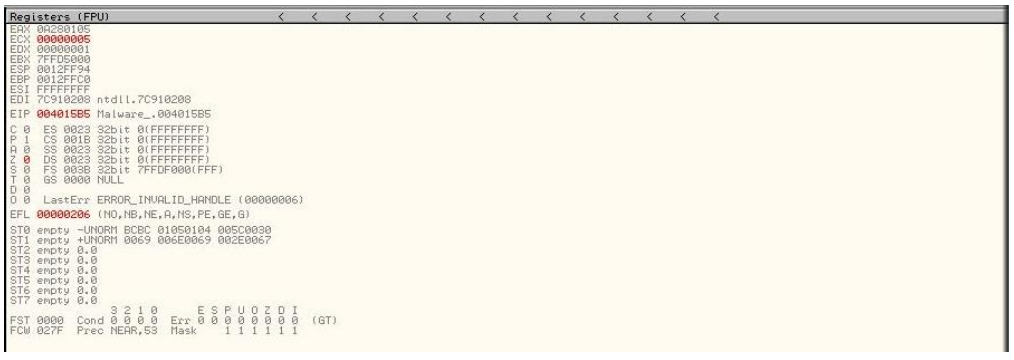
Individuiamo il nuovo indirizzo e inseriamo un toggle breakpoint come fatto precedentemente:



Il valore di ECX è pari a 0A280105:



Dopo l'operazione diventa 00000005:



L'istruzione eseguita è AND ECX, 0FF.

Il valore "0FF" sembra essere in esadecimale; l'istruzione AND ECX, 0FF sta effettuando un'operazione AND a livello bit tra il registro ECX e il valore esadecimale "0FF".

"0FF" in binario sarebbe "000011111111" (8 bit con tutti i bit da 1). Quindi, l'operazione di AND con "0FF" ha l'effetto di mantenere solo i primi 8 bit meno significativi di ECX, azzerando tutti gli altri bit.

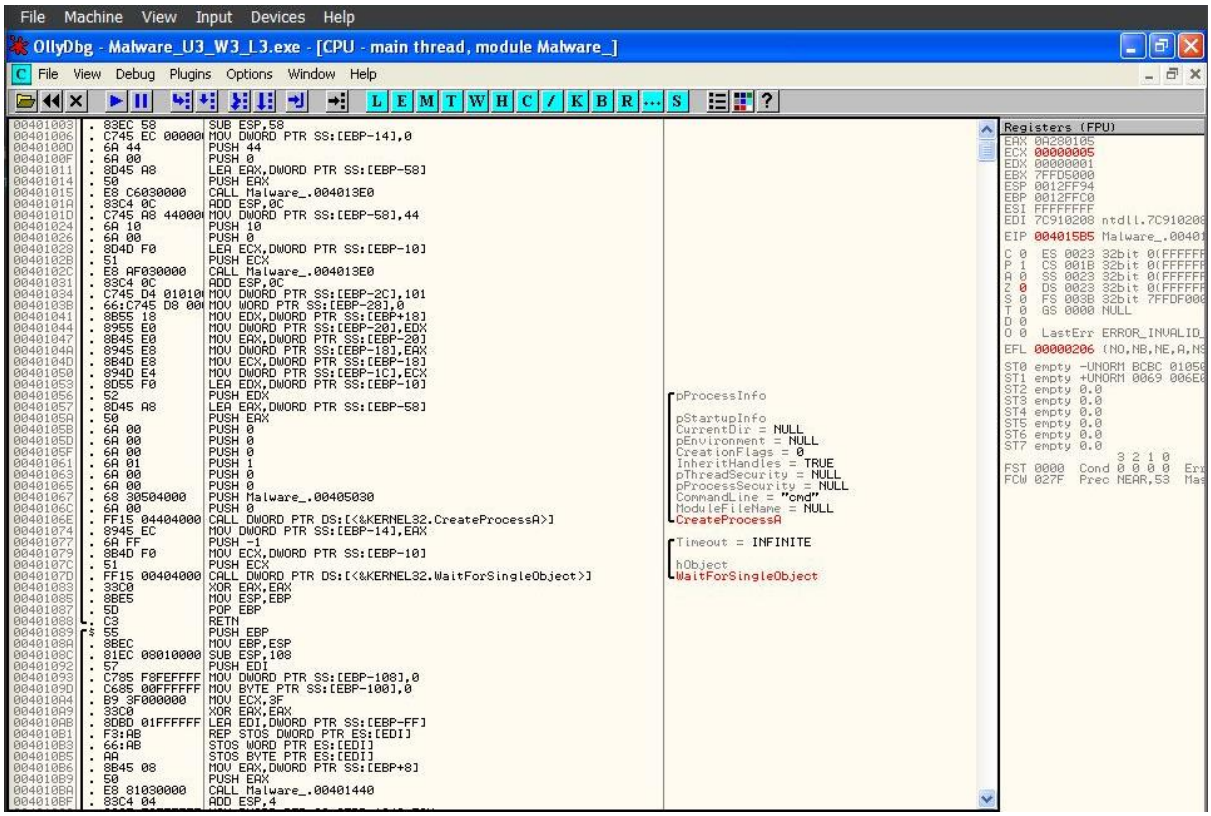
Considerato il valore iniziale di ECX "0A280105" (ad esempio, in binario: "00001010001010000001000000000101"), l'operazione di AND con "0FF" produce il risultato "00000000000000000000000000000101" (che è 5 in decimale).

QUESITO 4 - BONUS

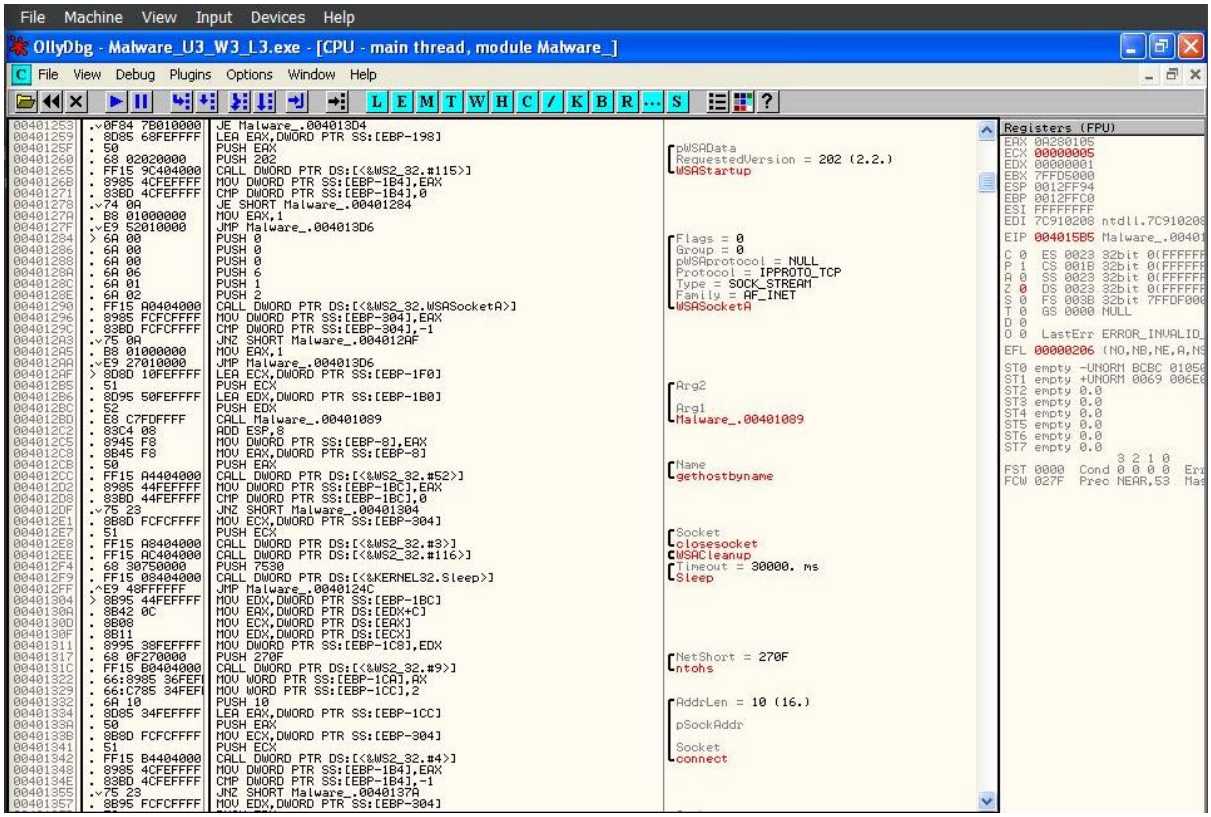
Spiegare a grandi linee il funzionamento del malware

Scorrendo il flusso del programma, è possibile distinguere la presenza di funzioni come chiamate di rete, manipolazione di stringhe, gestione della memoria e funzioni legate all'interfaccia utente.

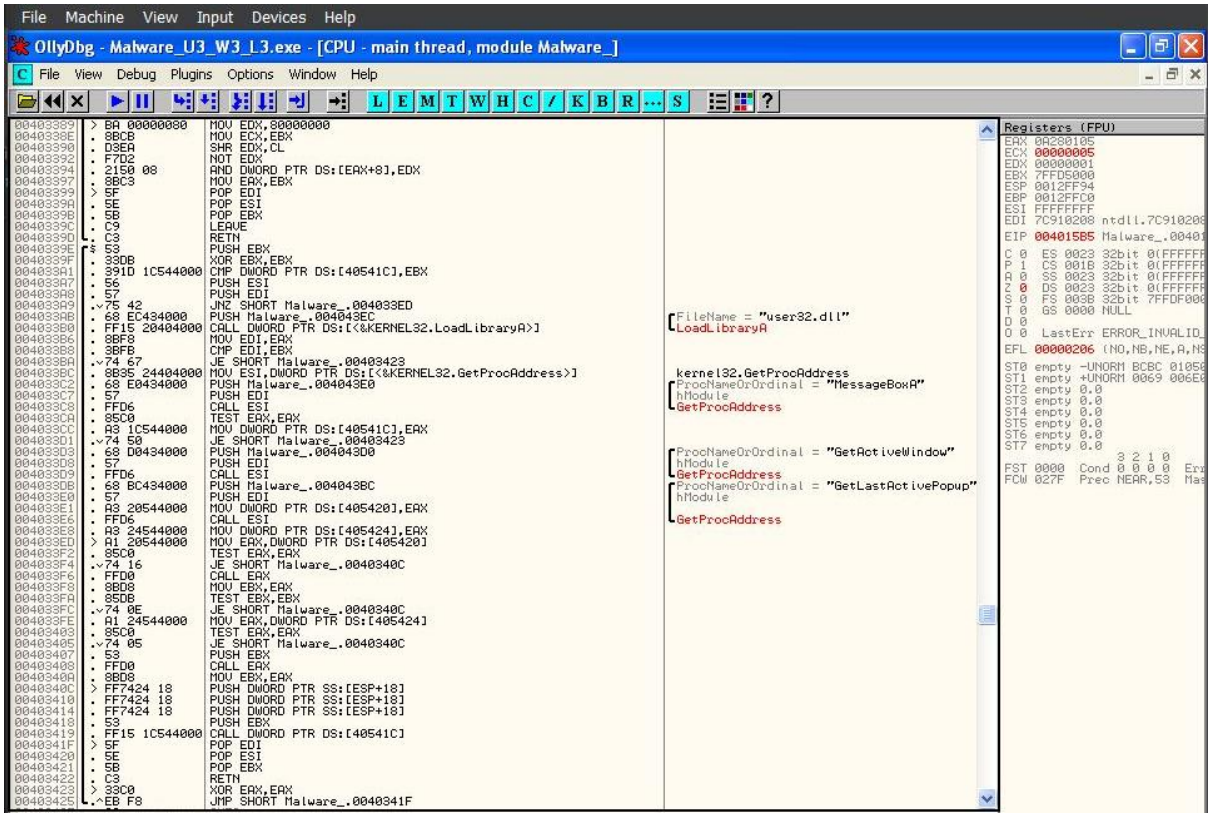
In questo punto, ad esempio, il malware crea un processo:



Qui crea un socket per connettersi con un server remoto:



Invece, l'uso delle funzioni presenti nello screenshot di seguito potrebbe indicare un tentativo di creare o manipolare elementi dell'interfaccia utente, come visualizzare messaggi pop-up ingannevoli o fuorvianti, ad esempio falsi messaggi di errore o notifiche per ingannare gli utenti affinché compiano determinate azioni o per creare una distrazione:



Tutto questo potrebbe indicare un malware multifunzionale in grado di eseguire varie attività. Inoltre, l'uso di tecniche di offuscamento, crittografia o tecniche anti-analisi potrebbe suggerire un tentativo di eludere la rilevazione.

Convertendo la firma in hash con MD5DEEP e cercandola con l'aiuto di Virus Total, quest'ultimo suggerisce che si possa trattare di un Trojan.