Traccia:

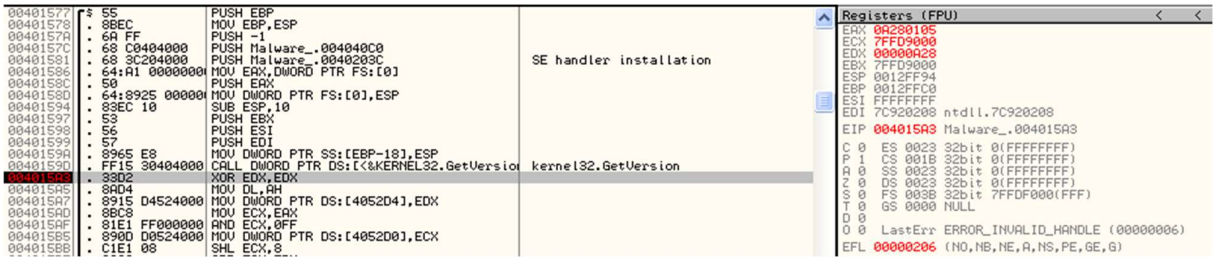
Fate riferimento al malware: **Malware_U3_W3_L3**, presente all'interno della cartella **Esercizio_Pratico_U3_W3_L3** sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

- 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 un 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

Tramite l'utilizzo del tool OllyDBG siamo riusciti a rispondere ai seguenti quesiti:

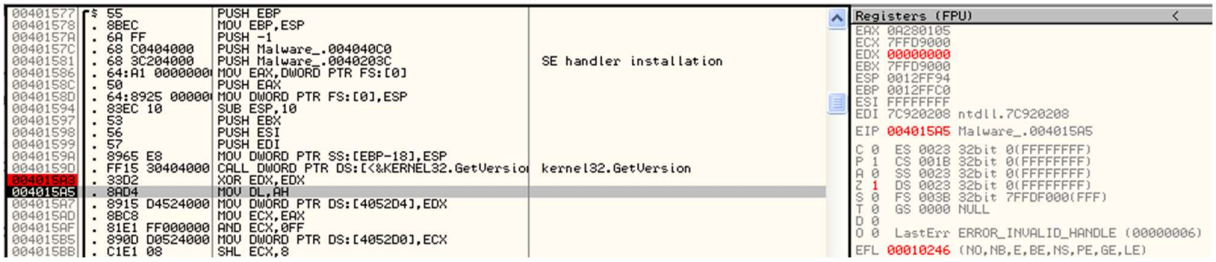
1) All'indirizzo 0040106E il valore del parametro Command Line è impostato su CMD come visibile in figura

2) Dopo aver inserito un Breakpoint all'indirizzo indicato, possiamo constatare che il valore del registro EDX è 00000A28

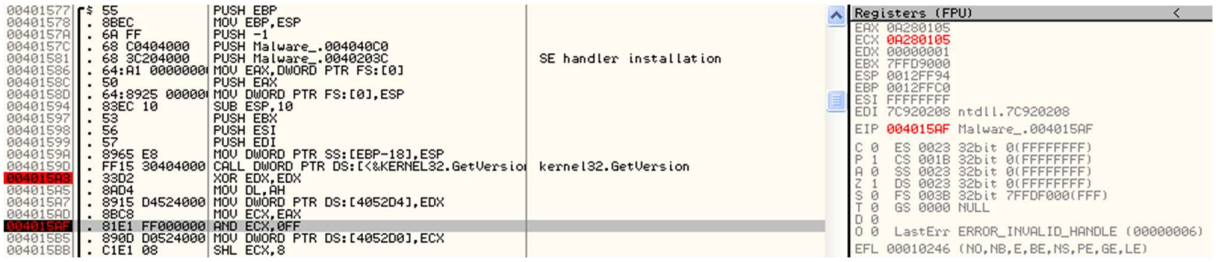


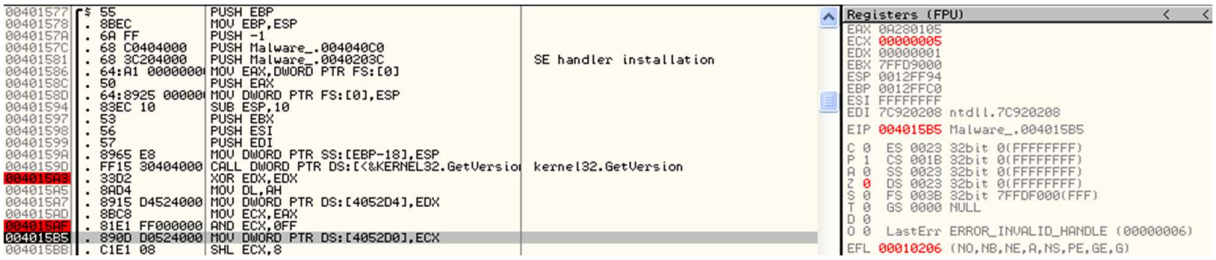
PRATICA S11/L3 – Giorgio Trovesi

1-4-5) Dopo aver eseguito uno “Step-Into” il valore del registro EDX è 00000000, questo perché viene eseguita l’istruzione XOR EDX,EDX che da come valore 0, perché lo XOR tra due valori uguali da come risultato sempre 0



6-7-8) Dopo aver inserito un Breakpoint all’indirizzo indicato il valore del registro ECX è 0A280105 e dopo aver eseguito uno “Step-Into” il valore è 00000005, perché è stata eseguita l’istruzione AND ECX,0FF che corrisponde all’esadecimale indicato.





BONUS) Tramite l’analisi del codice notiamo la presenza delle funzioni Socket e con l’utilizzo di VirtusTotal possiamo dedurre che si tratti di un Trojan che inserisce una backdoor nel sistema infettato