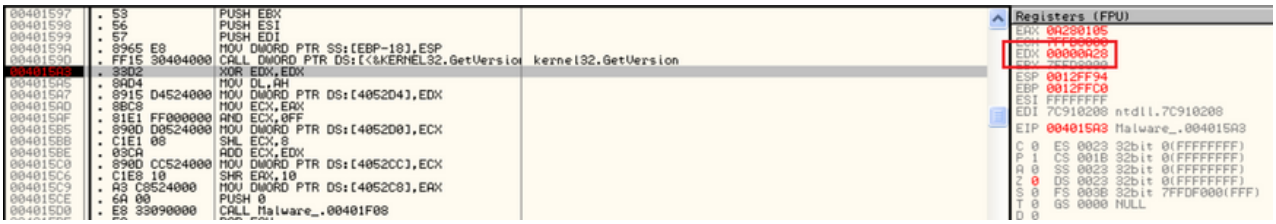
Esercizio S11 L3

Fate riferimento al malware: Malware_U3_W3_L3, presente all'interno della cartella Esercizio_Pratico_U3_W3_L3sul 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?

Il valore del parametro CommandiLine è: **cmd**

Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX?



Il valore del registro EDX è **00000A28**

Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?

Il valore del registro EDX ora è **00000000.** Lo step into viene tilizzato per esaminare righe di codice e a fronte di una chiamata di funzione accedere alla sua implementazione. In questo caso viene eseguita la riga di codice **XOR EDX, EDX** che è il comando per azzerare un registro.

Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX?

Il valore del registro ECX è **0A280105.**

Eseguite un step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.

Il valore di ECX è di **00000005** questo perchè viene eseguita una istruzione **AND** tra il registro ECX con valore 0A280105 e il valore **0FF** scritto in esadecimale. Il risultato di tale operazione è appunto 00000005.

BONUS: spiegare a grandi linee il funzionamento del malware.

Analizzando il comportamento del malware notiamo che crea processi in windows, crea file, prova ad nascondersi da strumenti di analisi, crea e si connette a TCP socket inoltre si comporta come un TCP client. Quindi potrebbe essere una reverse shell.