S11/L3

Traccia: 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.

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?
Vediamo che il parametro CommandLine è assegnato al valore "cmd" all'interno del programma, all'indirizzo 401067

2.Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX?
Eseguite a questo punto uno «step-into».

Il registro EDX contiene attualmente il valore 00000000, poiché è eseguita un'operazione XOR tra EDX e se stesso (EDX XOR EDX), il che restituisce sempre 0. Di conseguenza, il registro EDX viene inizializzato a zero

Indicate qual è ora il valore del registro EDX, motivando la risposta. Che istruzione è stata eseguita? Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? Eseguite un step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita:

Il valore di ECX iniziale e 7FFDF000.Al secondo breakpoint, notiamo che il valore è 0A280105. Dalle istruzioni nel codice assembly, osserviamo che il contenuto di EAX viene trasferito in ECX e successivamente viene eseguita un'operazione AND tra ECX e 0FF. Se l'operazione restituisce un risultato vero, il valore di ECX viene modificato