Esercizio Epicode 06.12.2023

Ollydbg

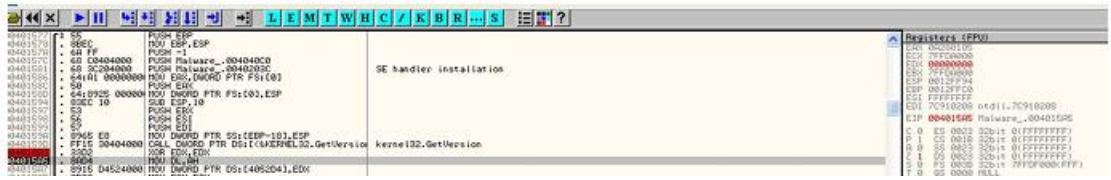
Con riferimento al Malware_U3_W3_L3, presente all'interno della cartella Esercizio_Pratico_U3_W3_L3. Rispondere ai seguenti quesiti utilizzando OllyDBG.

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 è «CMD» ovvero il command prompt di Windows, come si nota nella figura sottostante all'indirizzo 00401067

Inserire un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? Eseguire uno «step-into». Indicare qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?

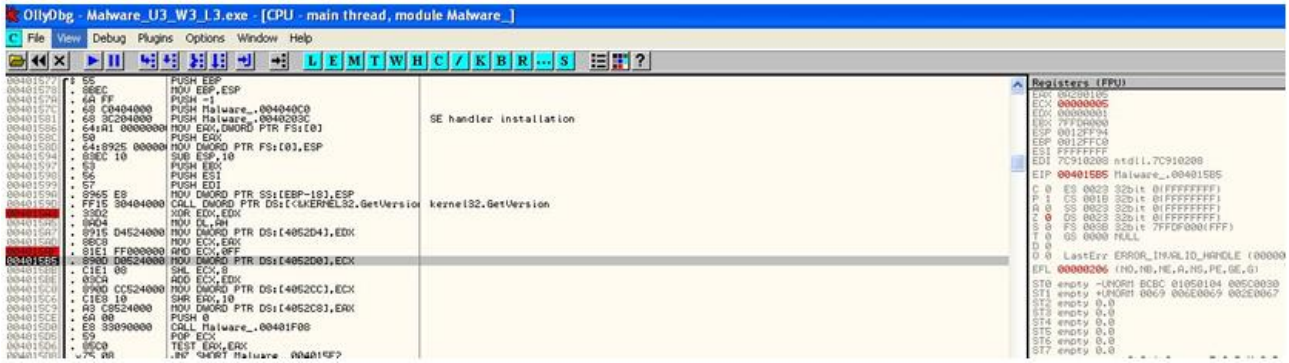
Una volta configurato il breakpoint, clicchiamo su «play», il programma si fermerà all'istruzione XOR EDX,EDX. Prima che l'istruzione venga eseguita il valore del registro è «00000A28». Dopo lo step-into, viene eseguita l'istruzione XOR EDX,EDX che di fatto equivale ad inizializzare a zero una variabile. Quindi, dopo lo step-into il valore di EDX sarà 0.



Inserire un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? Eseguire uno step-into. Qual è ora il valore di ECX? Spiegare quale istruzione è stata eseguita.

Configuriamo il secondo breakpoint. Il valore del registro ECX è «0A280105».

dopo lo step-into il valore del registro ECX è stato modificato in «00000005» in quanto è stata eseguita l'istruzione AND ECX, FF



Nel dettaglio, l'istruzione esegue l'AND logico sui bit di EAX e del valore esadecimale FF. Per prima cosa portiamo entrambi i valori in formato binario e poi eseguiamo l'AND logico tra i bit.

Esadecimale	Binario
0A280105	0000 1010 0010 1000 0000 0001 0000 0101
FF	0000 0000 0000 0000 0000 0000 1111 1111
Eseguendo l'AND logico tra i bit uno ad uno	0000 0000 0000 0000 0000 0000 0000 0101

Che in Esadecimale è 00000005

Ecco spiegato il valore di ECX dopo l'istruzione AND ECX, 0FF