S11/L3 Esercizio 06/12/2023

Nell'esercizio di oggi ci viene richiesto, in base al malware fornito, di rispondere ai seguenti quesiti usando OllyDBG:

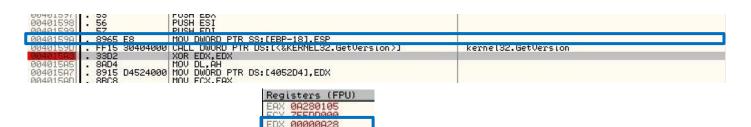
- Qual è il valore del parametro «CommandLine» che viene passato sullo stack all'indirizzo 0040106E
- Inserire un breakpoint software all'indirizzo 004015A3 e dire qual'è il valore del registro EDX
- Eseguire uno «step-into» e indicare a questo punto qual è ora il valore del registro EDX
- Motivare la risposta
- Spiegare quale istruzione è stata eseguita
- Inserire un secondo breakpoint all'indirizzo di memoria 004015AF e dire qual'è il valore del registro ECX
- Eseguite uno step-into e dire qual è ora il valore di ECX
- Spiegare quale istruzione è stata eseguita
- BONUS: spiegare a grandi linee il funzionamento del malware

Quesito 1

Come possiamo vedere dall'immagine il valore del parametro "CommandLine" che viene passato sullo stack è "cmd"

Quesito 2

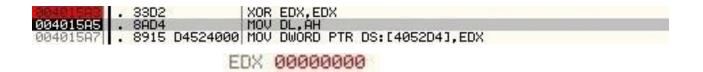
Dopo aver inserito il breakpoint software attraverso i comandi <<tasto dx/Breackpoint/Toogle>> e aver avviato il programma possiamo rilevare il valore EDX 00000A28



0012FF94

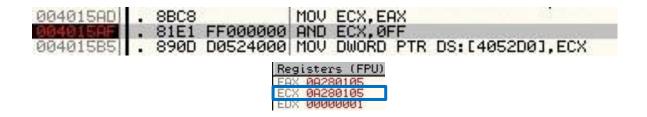
Quesito 3-4-5

Eseguendo uno "step-into" con il comando il valore EDX viene azzerato, questo perché l'istruzione "XOR EDX, EDX" è comunemente utilizzata per azzerare il registro confrontando con la funzione "XOR" tutti i bit presenti dando 0 come risultato nel caso risultino uguali e 1 nel caso fossero diversi



Quesito 6

Dopo aver inserito il breakpoint software possiamo rilevare il valore ECX 0A280105



Quesito 7-8

Eseguendo uno "step-into" il valore ECX diventa 00000005. L'istruzione AND ECX, 0FF "maschera" tutti i bit tranne gli ultimi 8 bit in ECX, il risultato sarà che solo l'ultimo byte di ECX sarà mantenuto, mentre gli altri byte verranno azzerati.



Quesito BONUS

Analizzando altre linee di codice troviamo la dicitura "call" su Socket Connect quindi potremmo ipotizzare che ci troviamo davanti ad una backdoor client