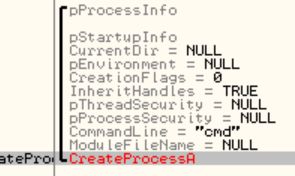
Esercizio 3 Settimana 11

Oggi andremo a fare pratica con il programma OllyDBG, usando un malware come esempio andremo e rispondendo alle seguenti domande:

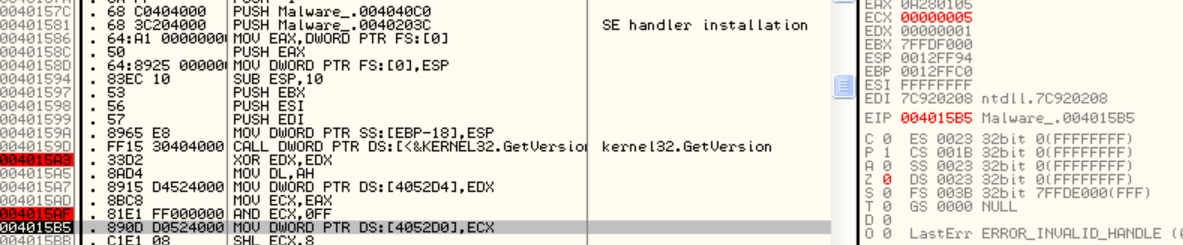
1. All’indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack?
2. Inserite un breakpoint software all’indirizzo 004015A3. Qual è il valore del registro EDX?
3. Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?
4. Inserite un secondo breakpoint all’indirizzo di memoria 004015AF. Qual è il valore del registro ECX?
5. Eseguite un step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.

Per rispondere alla domanda 1, basterà andare all’indirizzo di memoria sopra citato e controllare qual è il parametro di CommandLine. Questo sarà il risultato:

potremo vedere che il valore del parametro risulta essere cmd.

Passando alla seconda domanda, andremo all’indirizzo 004015A3 e procederemo ad inserire un breakpoint. Il valore del registro EDX sarà uguale a 0, come da figura sottostante:

Per far si che il registro sia uguale a 0, abbiamo effettuato uno step into una volta inserito il breakpoint. Facendo questo, verrà eseguito lo XOR e quindi il valore di EDX sarà uguale a 0.

Proseguendo, la domanda successiva ci chiede di inserire un secondo breakpoint all’indirizzo 004015AF e successivamente di verificare quale sia il valore di ECX.

Come possiamo notare, il valore di ECX sarà uguale a 5.