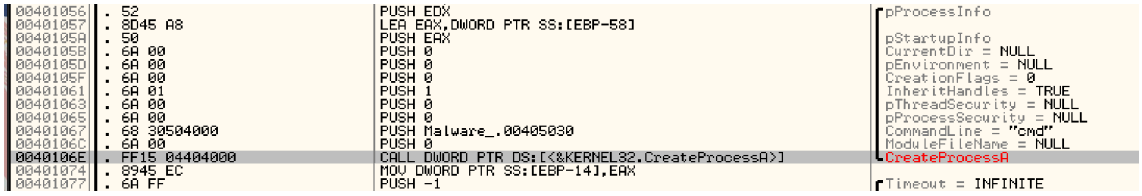
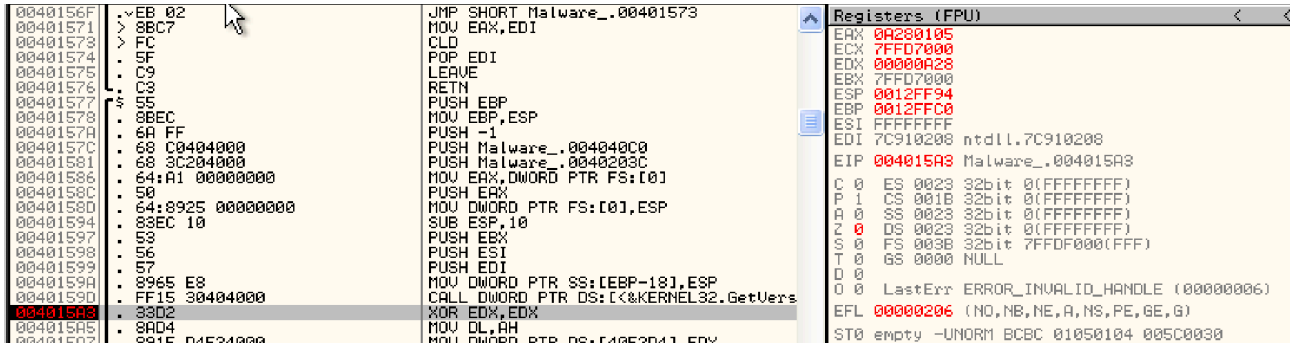
3. Malware analysis: Analisi dinamica avanzata

- 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?



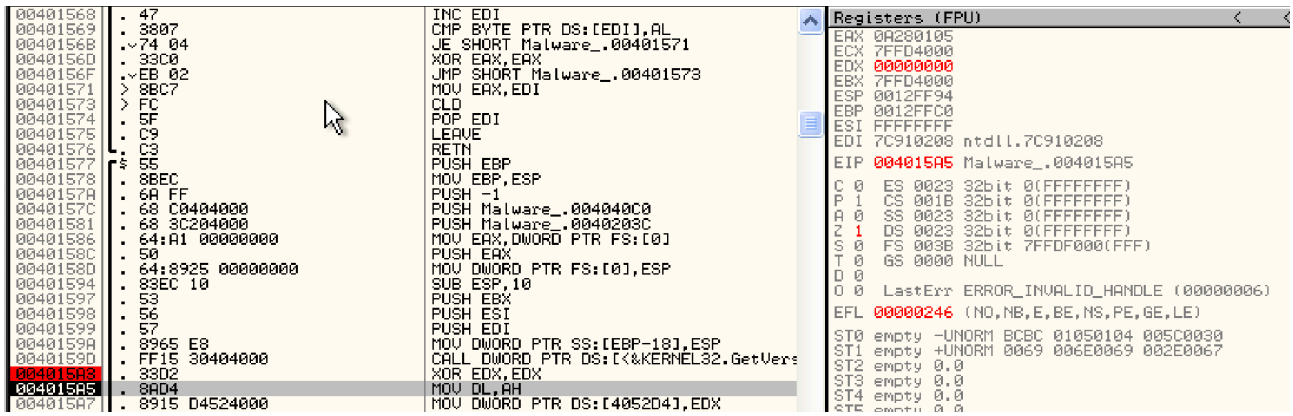
Come si nota dalla figura figura, il valore del parametro è **CMD** (comando prompt Windows).

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



Come da figura, il valore del registro EDX è **00000A28**.

- Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX.



Il valore di EDX cambia, come è possibile vedere in figura, con il valore 0.

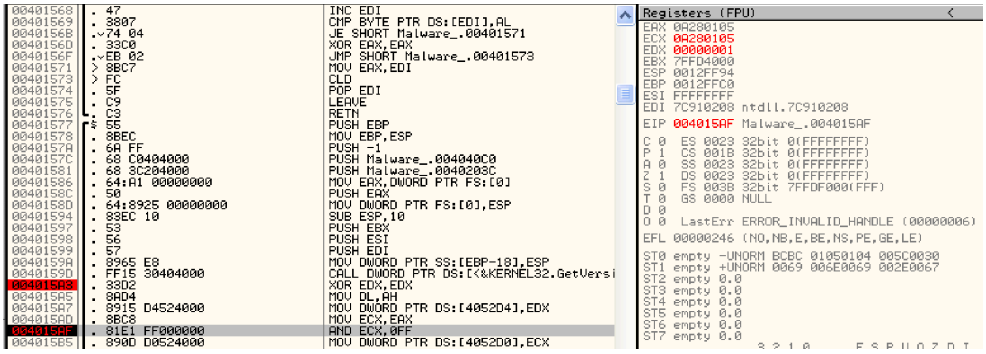
- Motivazione della risposta.

Configurando il brackpoint e premendo play, il programma si ferma all'istruzione XOR, dove troviamo il valore 00000A28 prima dell'esecuzione dell'istruzione. Successivamente attraverso lo step-info viene eseguita l'istruzione che è equivalente ad inizializzare a 0 una variabile. In questo caso, il valore di EDX sarà 0.

- Che istruzione è stata eseguita?

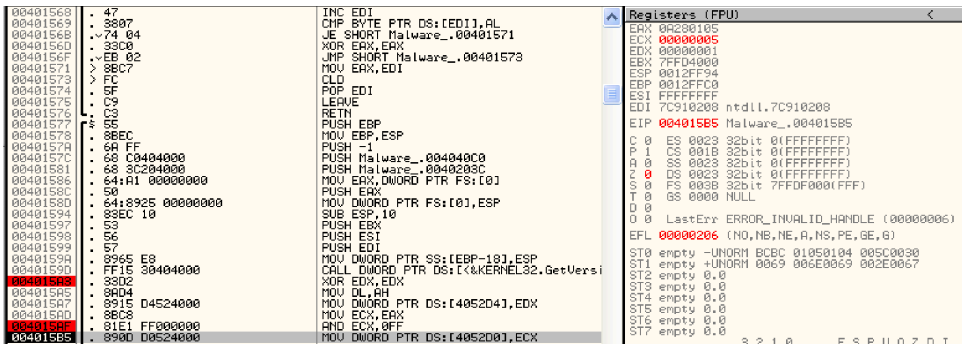
Viene eseguita l'istruzione XOR EDX,EDX

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



Il valore del registro ECX in questo caso è **0A280105**.

Eseguite un step-into. Qual è ora il valore di ECX?



Ora il valore di ECX è cambiato con **00000005**.

- Spiegate quale istruzione è stata eseguita.

Viene eseguita l'istruzione AND sui bit ECX ed il valore FF (esadecimale).
Convertiamo i valori in forma binaria ed eseguiamo l'AND logico.

0A280105 0000 1010 0010 1000 0000 0001 0000 0101
FF 0000 0000 0000 0000 0000 0000 1111 1111

AND logico 0000 0000 0000 0000 0000 0000 0000 0101
Che corrisponde all'esadecimale 00000005.

In questo modo possiamo capire il valore di ECX dopo l'istruzione.

- **BONUS: spiegare a grandi linee il funzionamento del malware**

Il malware è una reverse Shell