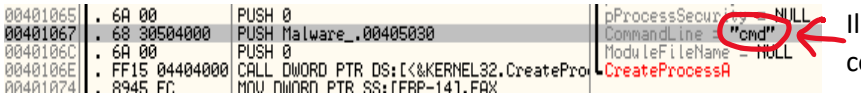
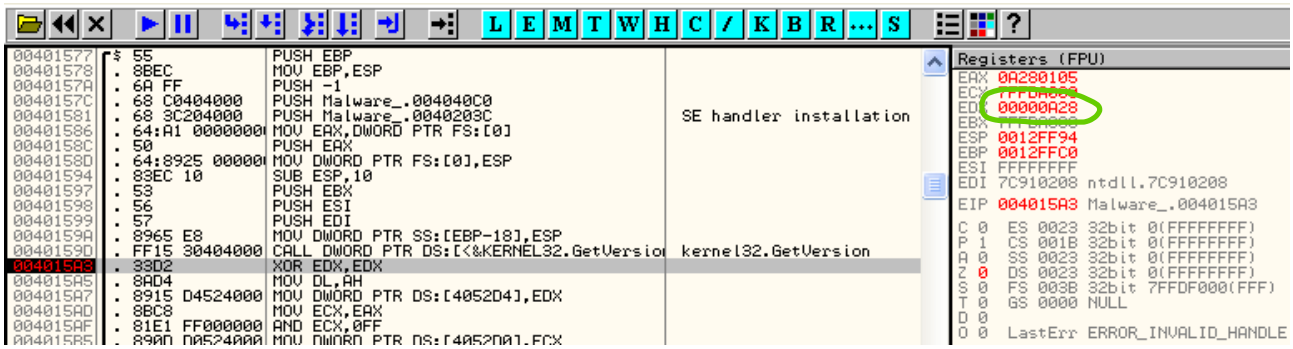
Valore del parametro «CommandLine»

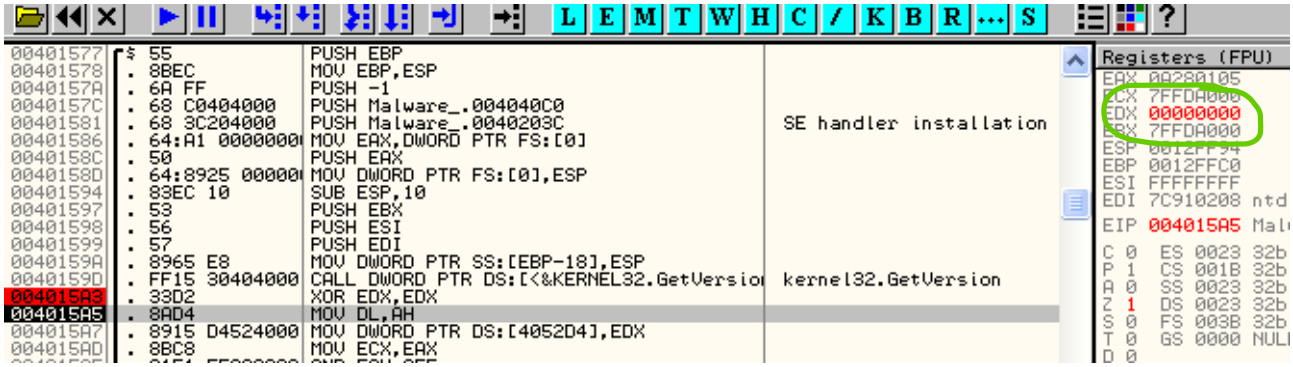


Il Valore del parametro è il prompt dei comandi di Windows.

Primo Breakpoint

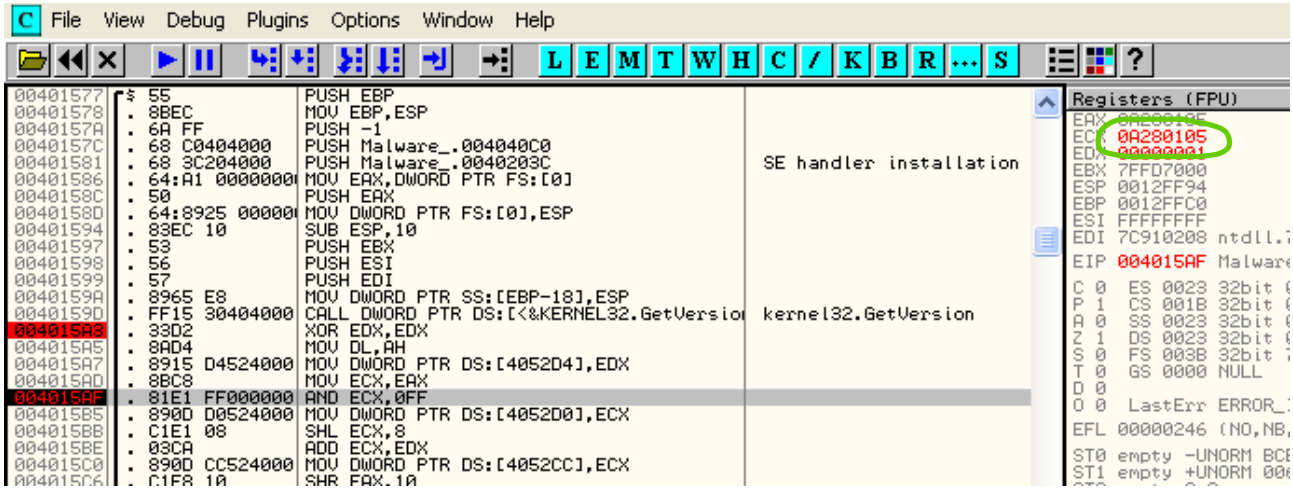


Dopo aver configurato il breakpoint e cliccando play, il programma si ferma all'indirizzo 004015A3. Il valore è 00000A28. Una volta eseguito lo step-into, il valore di EDX è uguale a 0.

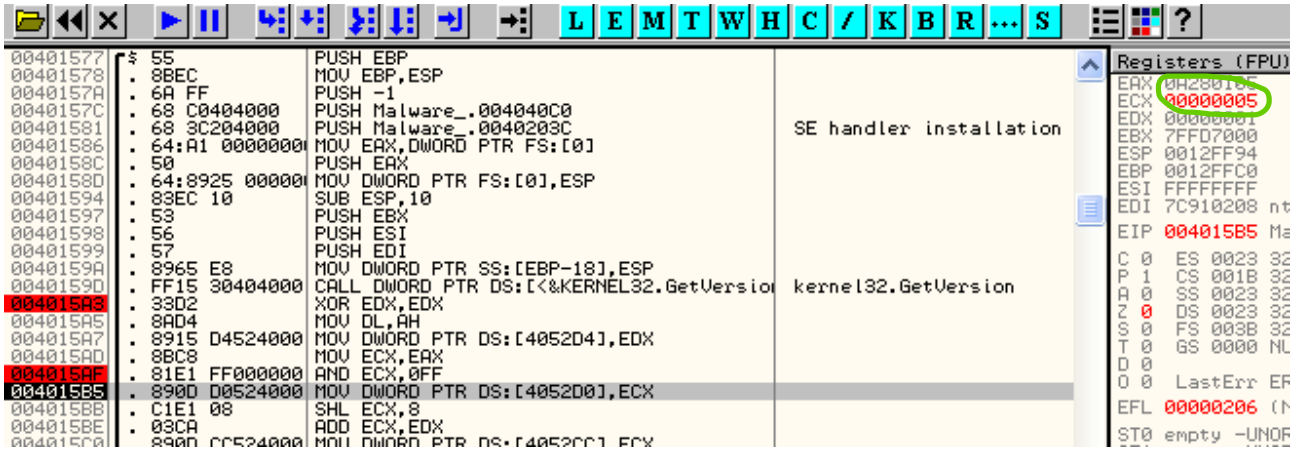


L'istruzione eseguita è XOR EDX,EDX.

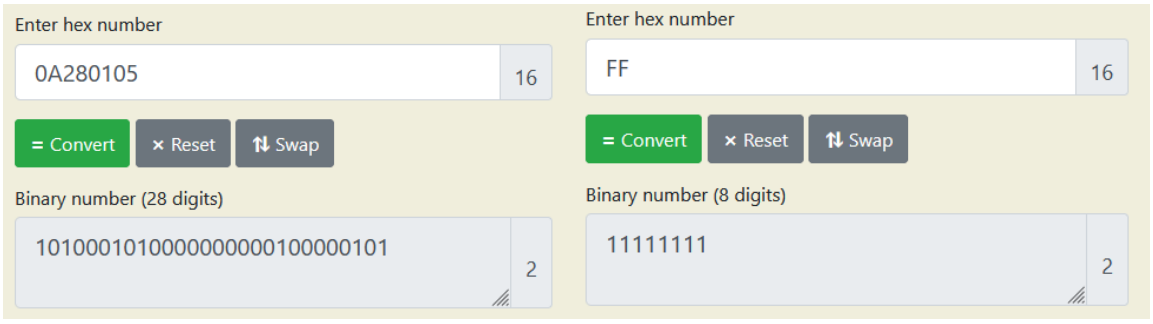
Secondo Breakpoint



Dopo aver configurato il breakpoint e cliccando play, il programma si ferma nuovamente all'indirizzo 004015AF. Il valore è 0A280105. Una volta eseguito lo step-into, il valore di ECX è uguale a 00000005.



L'istruzione eseguita è AND ECX,OFF.



Eseguendo l'AND tra i due valori otteniamo 00000000000000000000000000101 che in esadecimale è 5

Malware

Il codice dovrebbe essere una reverse shell, dato che il cmd viene processato e rimane sempre in background. Il malware dovrebbe inizializzare la comunicazione di rete, connettendosi a un server in una determinata porta e controlla se l'operazione ha avuto successo ripetendo il loop.

Il file deve essere rinominato in ocl per poter essere avviato.

Il programma fa una comparazione per poter proseguire l'esecuzione. Se il file non è denominato appunto come "ocl.exe", il file si chiude.