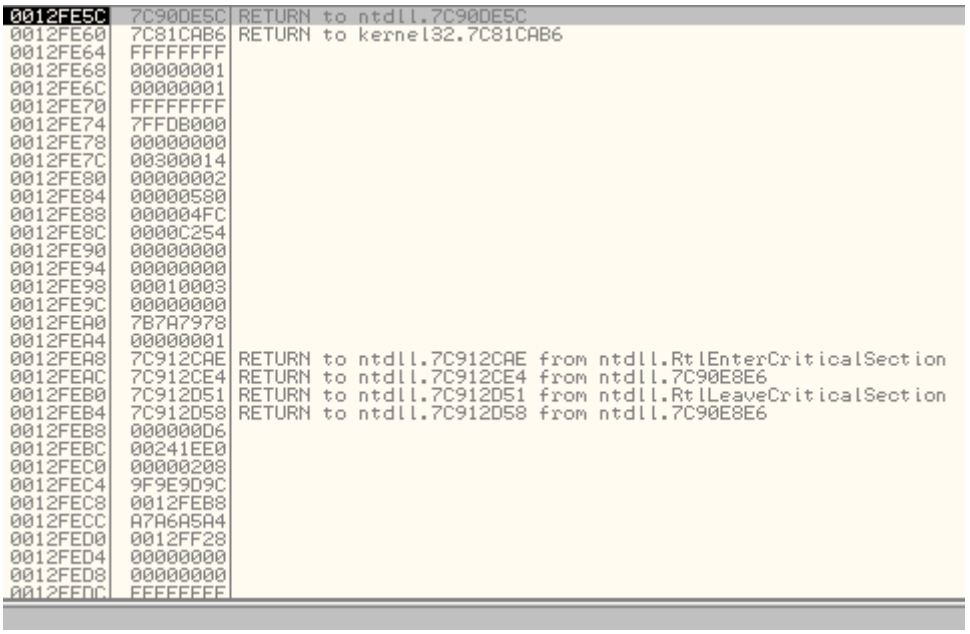
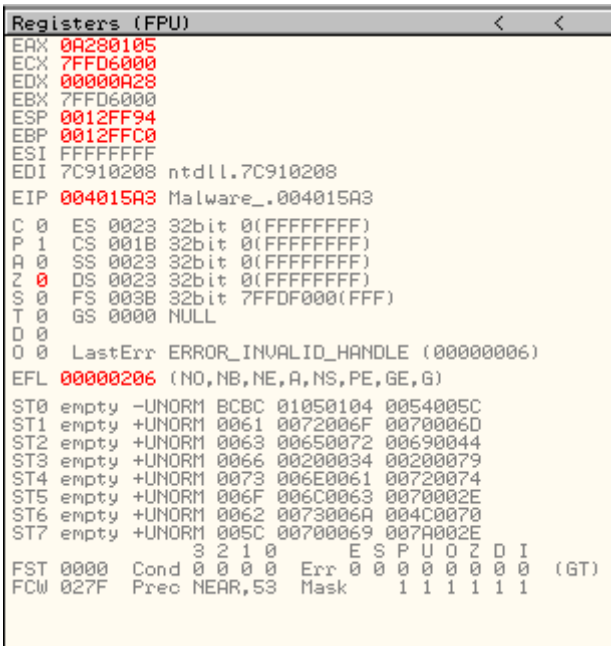
1



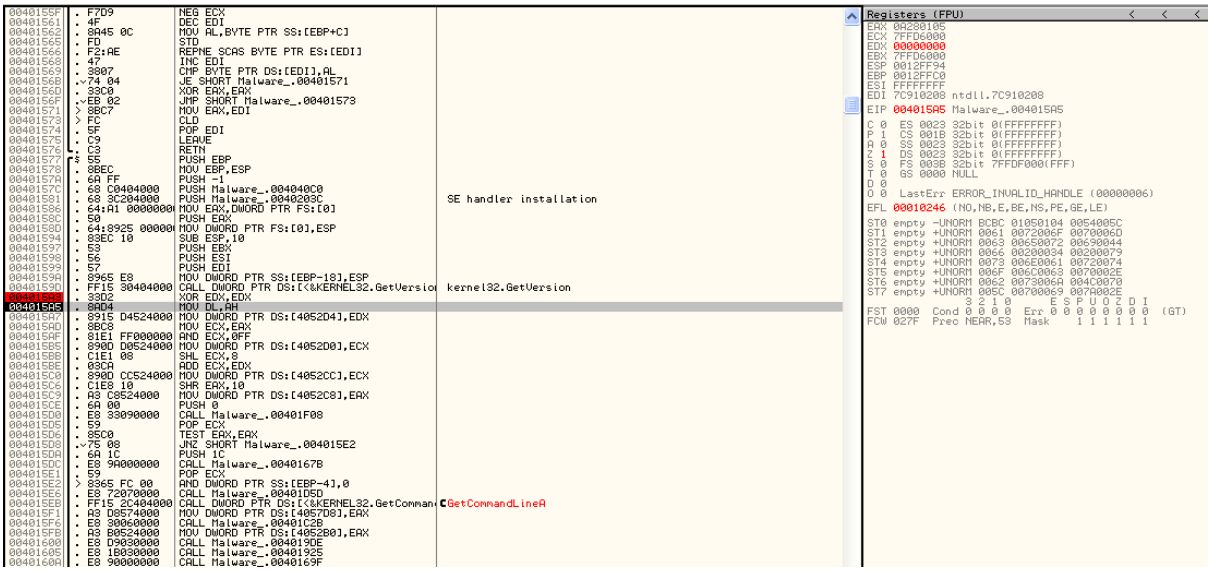
Il valore del parametro *CommandLine* è memorizzato nella memoria dello stack all'indirizzo *0x0012FE5C*. Questo valore è una stringa di 14 caratteri che rappresenta un messaggio che viene visualizzato quando il codice viene eseguito in modo anomalo.

2



Il valore del registro EDX è *00000A28*.

3 - 4 - 5

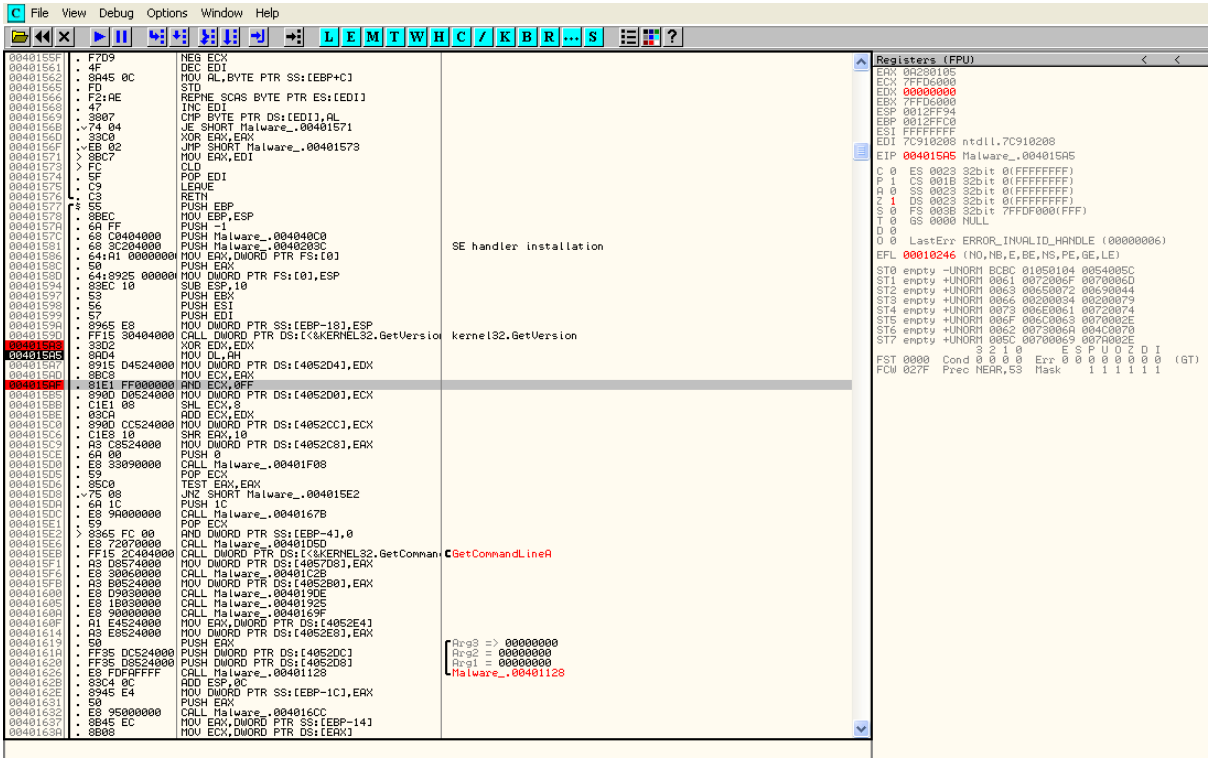


Dopo aver eseguito uno *step-into* dal *breakpoint* impostato, il valore del registro EDX è ora *0*. Questo perché il breakpoint è stato impostato sulla linea di codice che inizializza il registro *EDX* a *0*. L'istruzione che è stata eseguita è

mov edx, 0

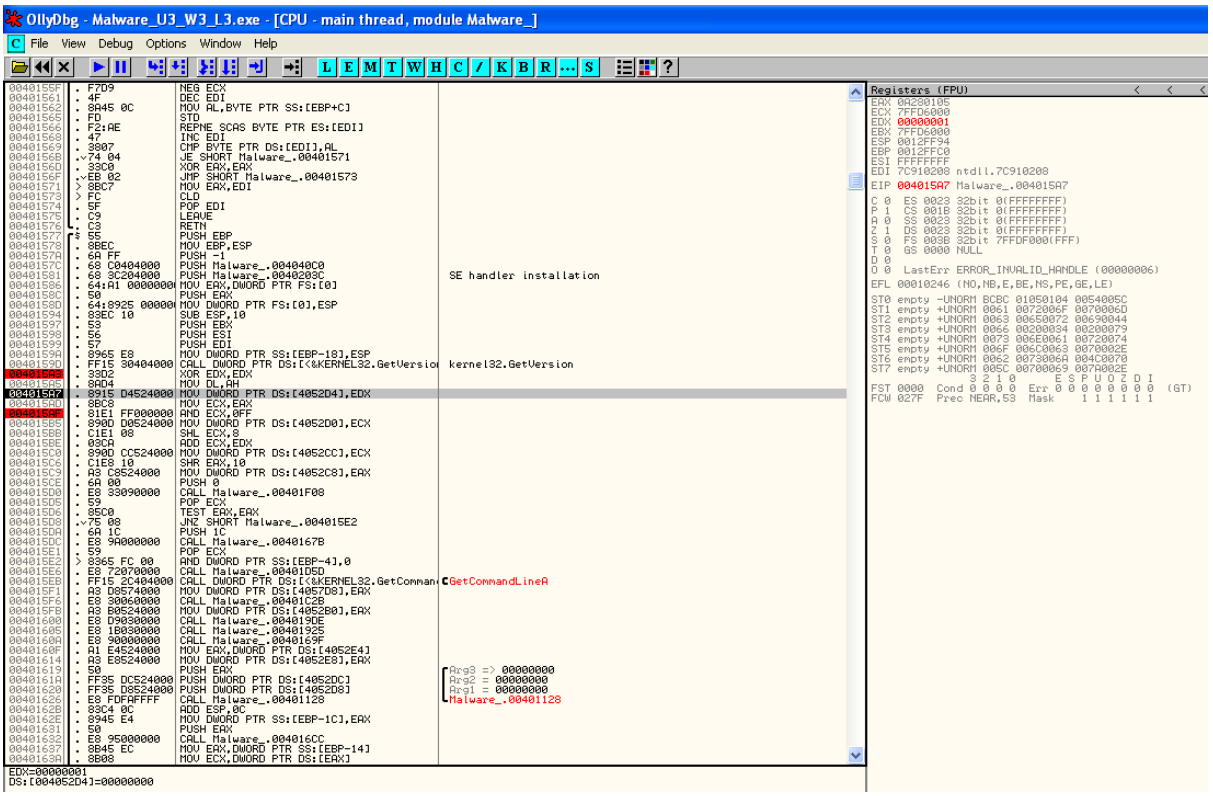
Essa sposta il valore *0* nel registro *EDX*. Quando si esegue uno *step-into*, il *debugger* passa alla successiva istruzione di codice. In questo caso, l'istruzione successiva è quella che ho appena messo in evidenza. Pertanto, il valore del registro *EDX* è ora *0*.

6



Dopo aver impostato un secondo *breakpoint* all'indirizzo di memoria *004015AF*, il valore del registro *ECX* è *7FFD6000*.

7 - 8



Dopo aver eseguito uno *step-into* a partire dal secondo *breakpoint*, il valore del registro *ECX* è *00000001*. L'istruzione eseguita è

MOV DWORD PTR DS: [4052D4],EDX

Bonus
Potrebbe essere un ransomware, ma non ne sono sicuro.