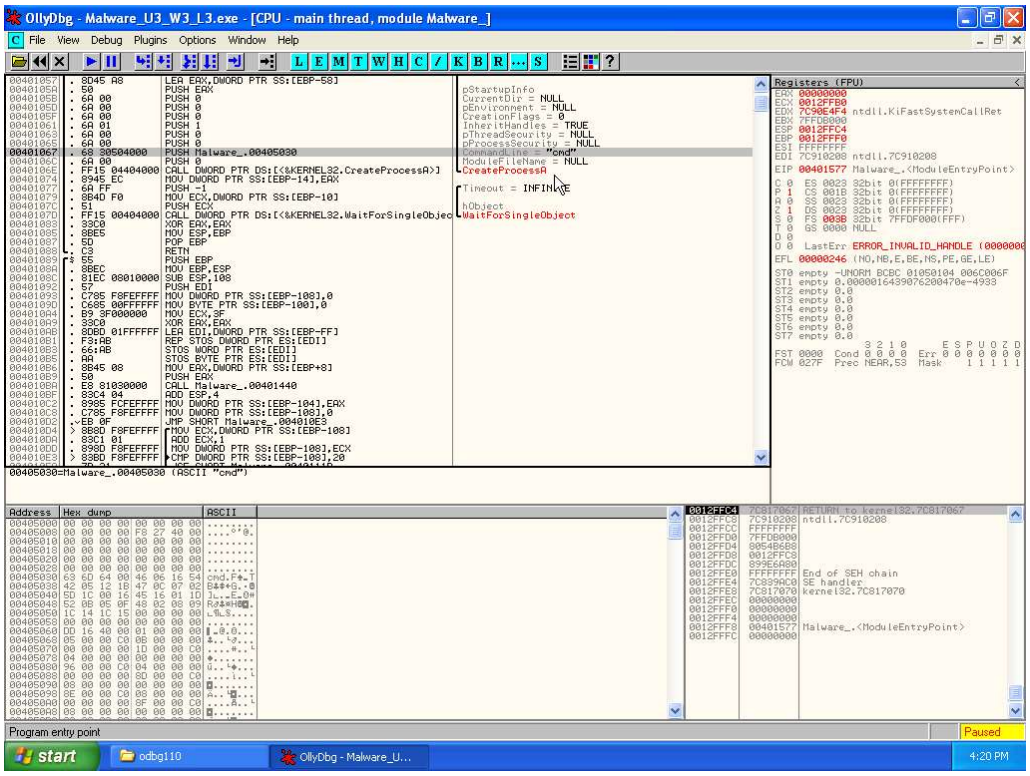
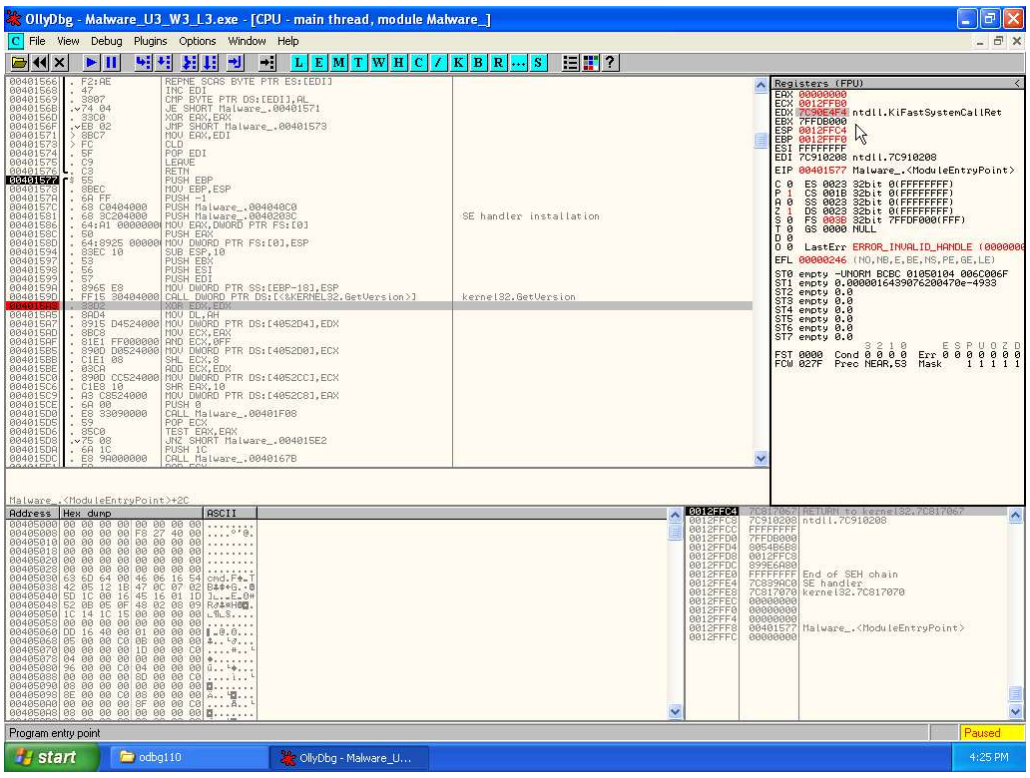
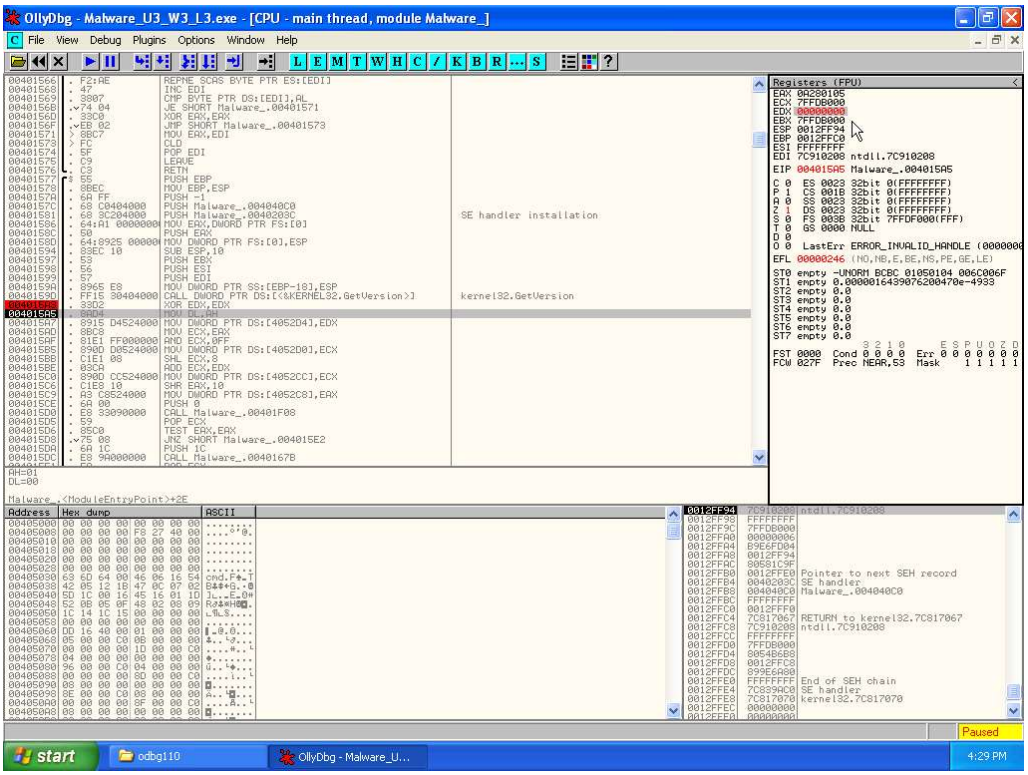


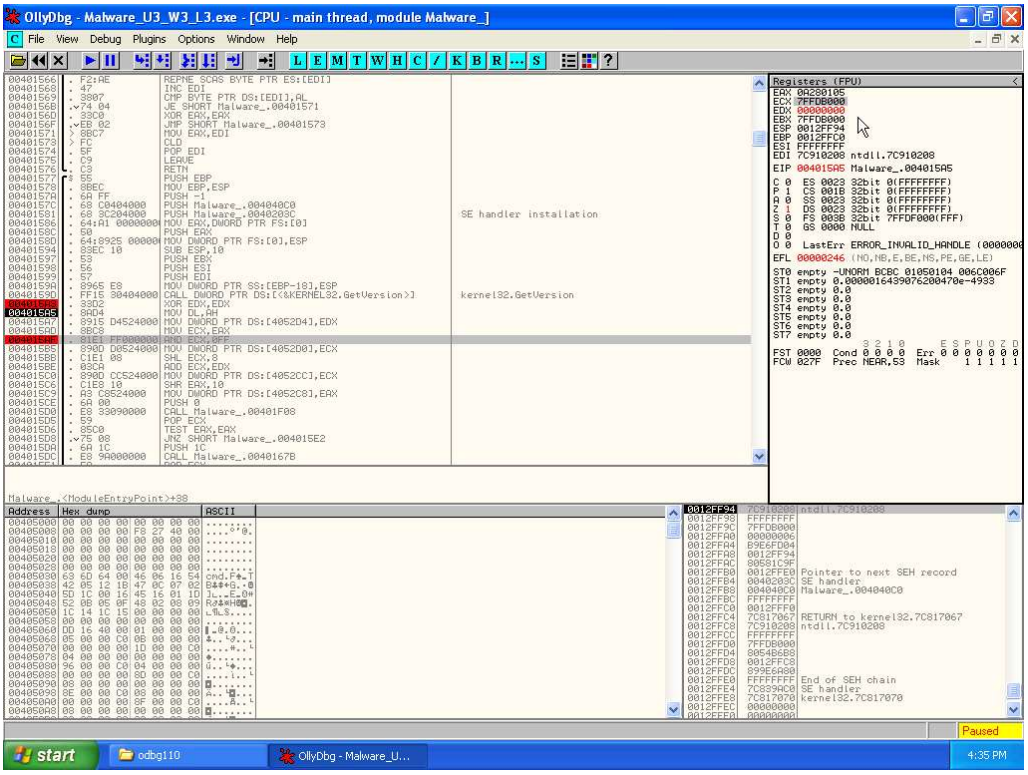

Il valore che viene passato sullo stack dal parametro **CommandLine** è **cmd** (indirizzo 00401067).



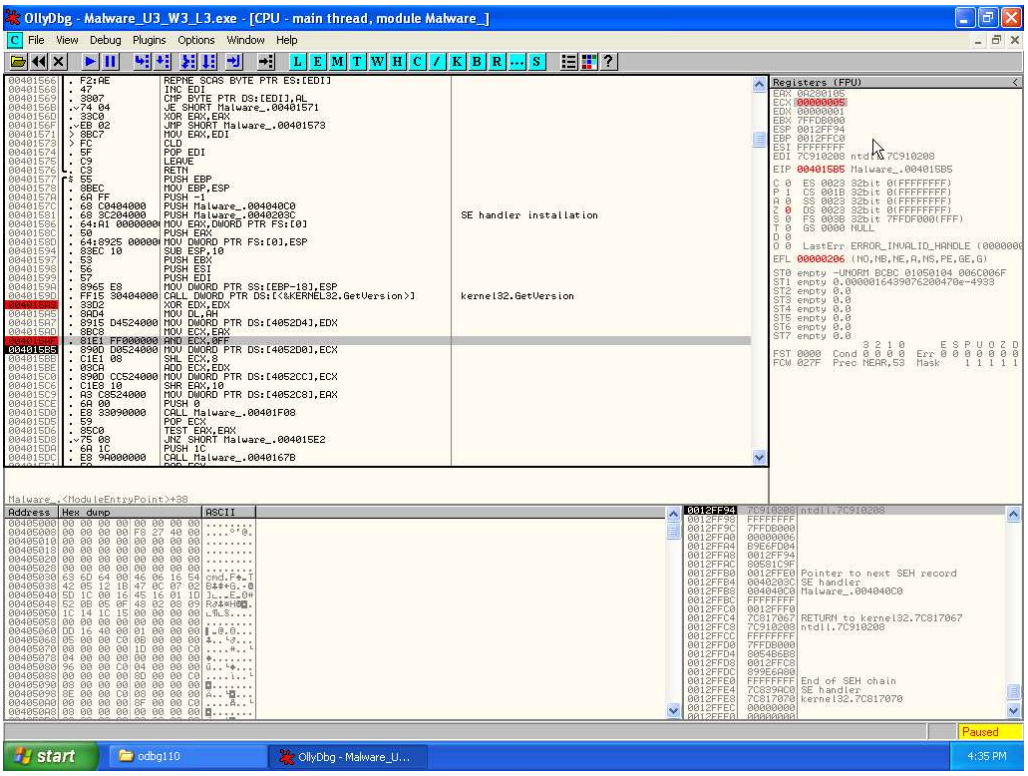

Il valore del registro **EDX** (indirizzo 004015A3) è **7C90EA4F4**.
Creiamo un **breakpoint** ed eseguiamo uno **step-into** e rincontrolliamo il valore del registro **EDX**.




Il nuovo valore è **00000000**. Questo perché lo **XOR** moltiplicato per se stesso non può che ritornare valore **0**.
Inseriamo un secondo **breakpoint** all'indirizzo **004015A3** e controlliamo il valore di **ECX**.




Annotiamo il valore (7FFDB000) e procediamo con uno step-into.
Notiamo che viene eseguita l'istruzione **AND ECX, OFF** ed il valore di **ECX** cambia in **00000001** che non è altro che il risultato del calcolo d'istruzione dei due esadecimali espresso in binario.


OllyDbg - Malware_U3_W3_L3.exe - [CPU - main thread, module Malware_]
File View Debug Plugins Options Window Help
Registers (FPU)
SE handler installation
kernel32.GetVersion
Paused
start
odbg110
OllyDbg - Malware_U...
4:35 PM