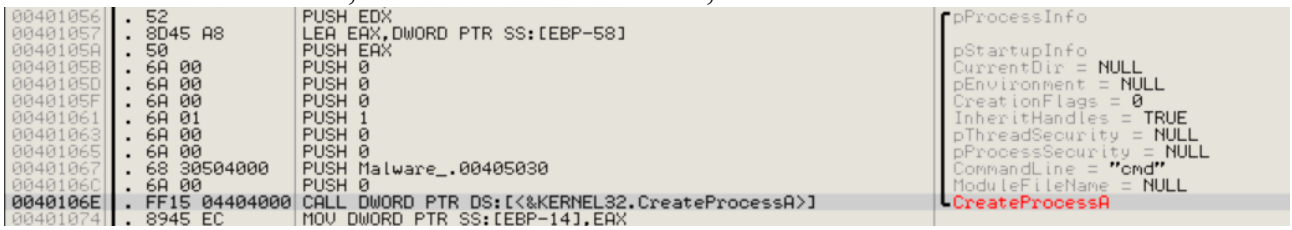
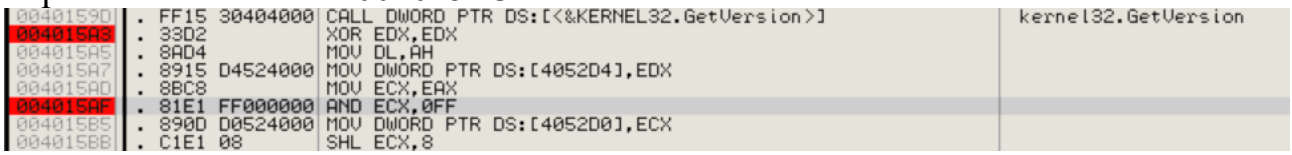
Analisi dinamica avanzata

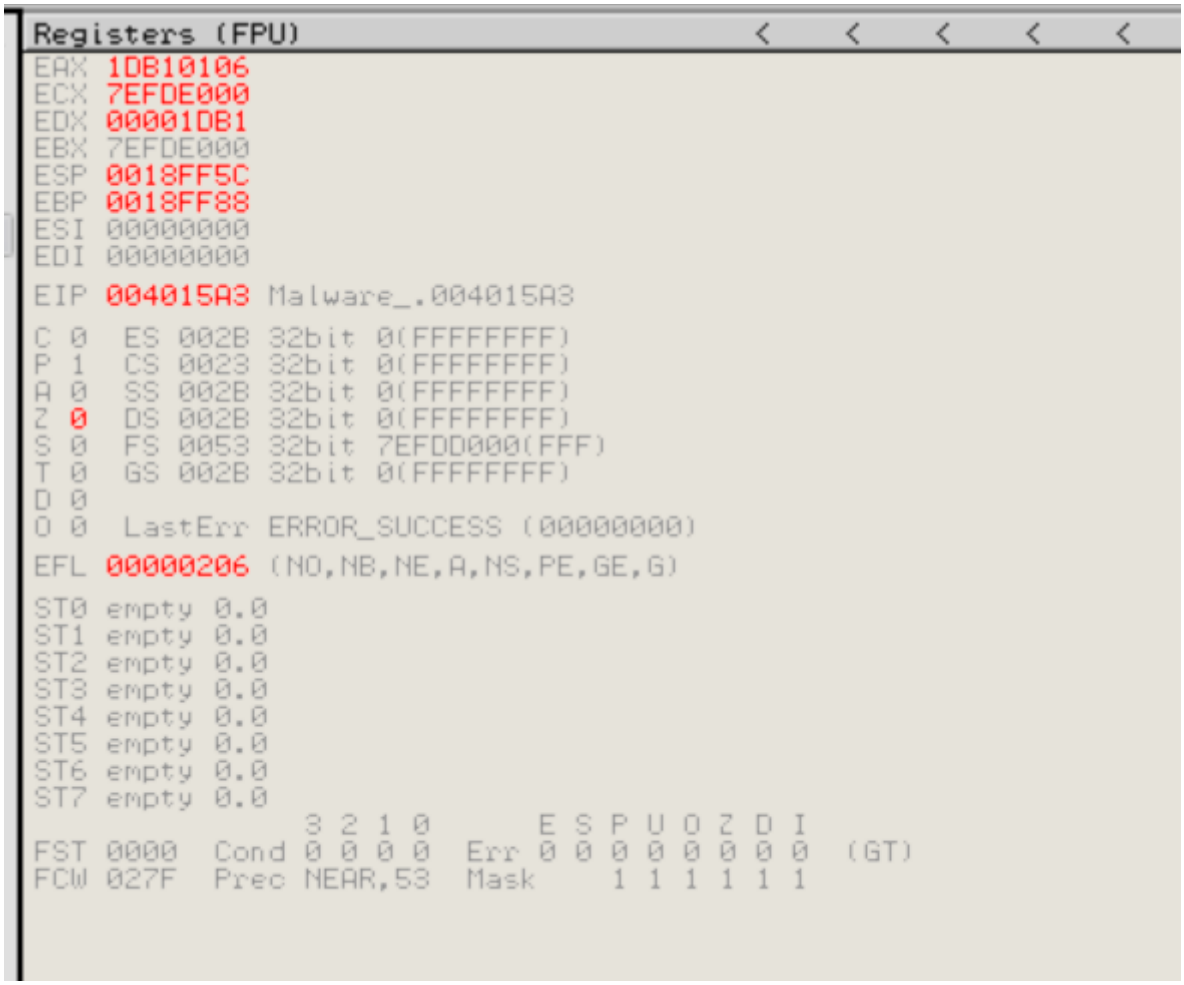
all'interno del malware, all'indirizzo 0040106E, troviamo il commandLine “cmd”



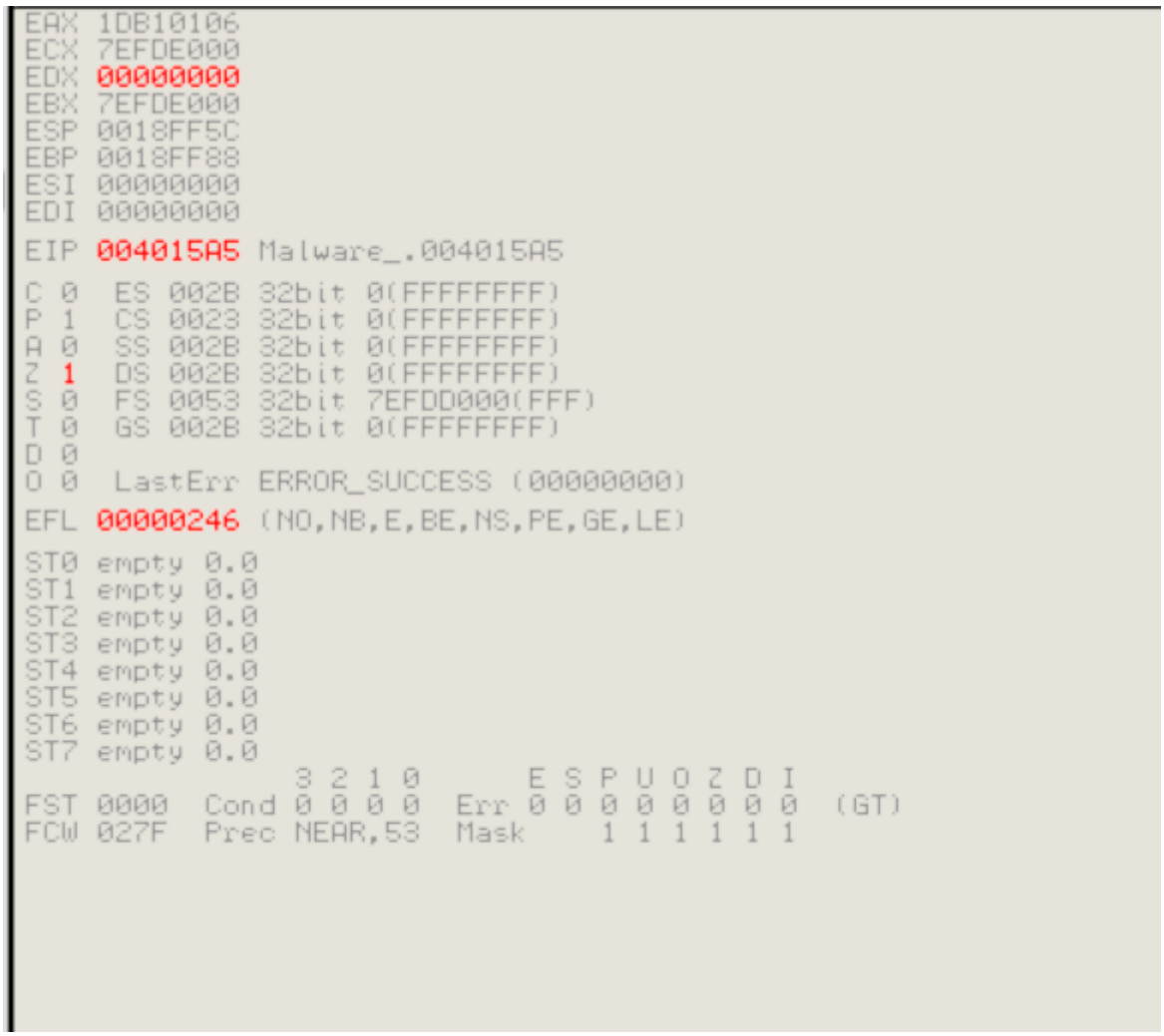
dopodiche all'indirizzo 004015A3



troviamo che il valore di edx inizialmente è

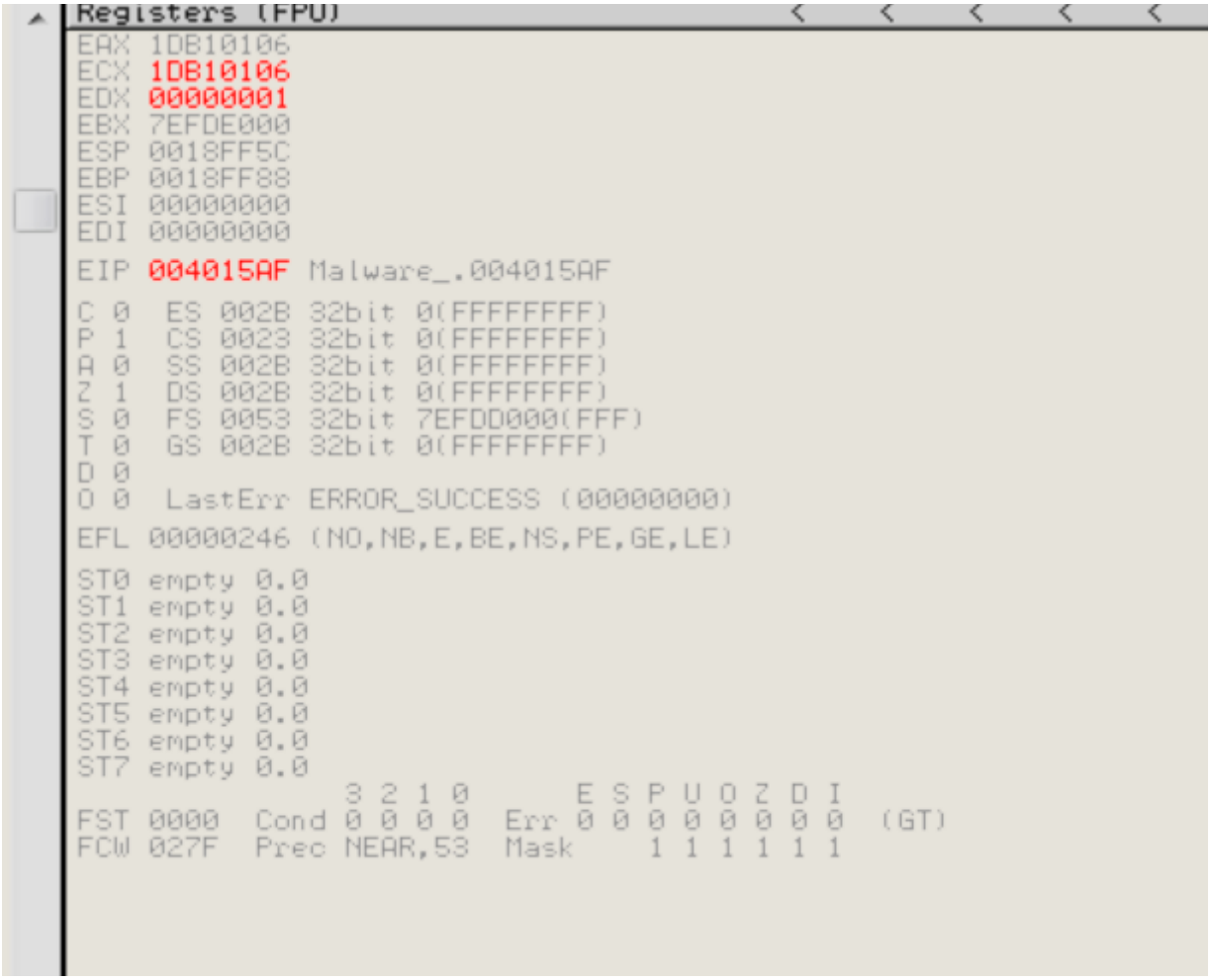


questo valore si modifica in

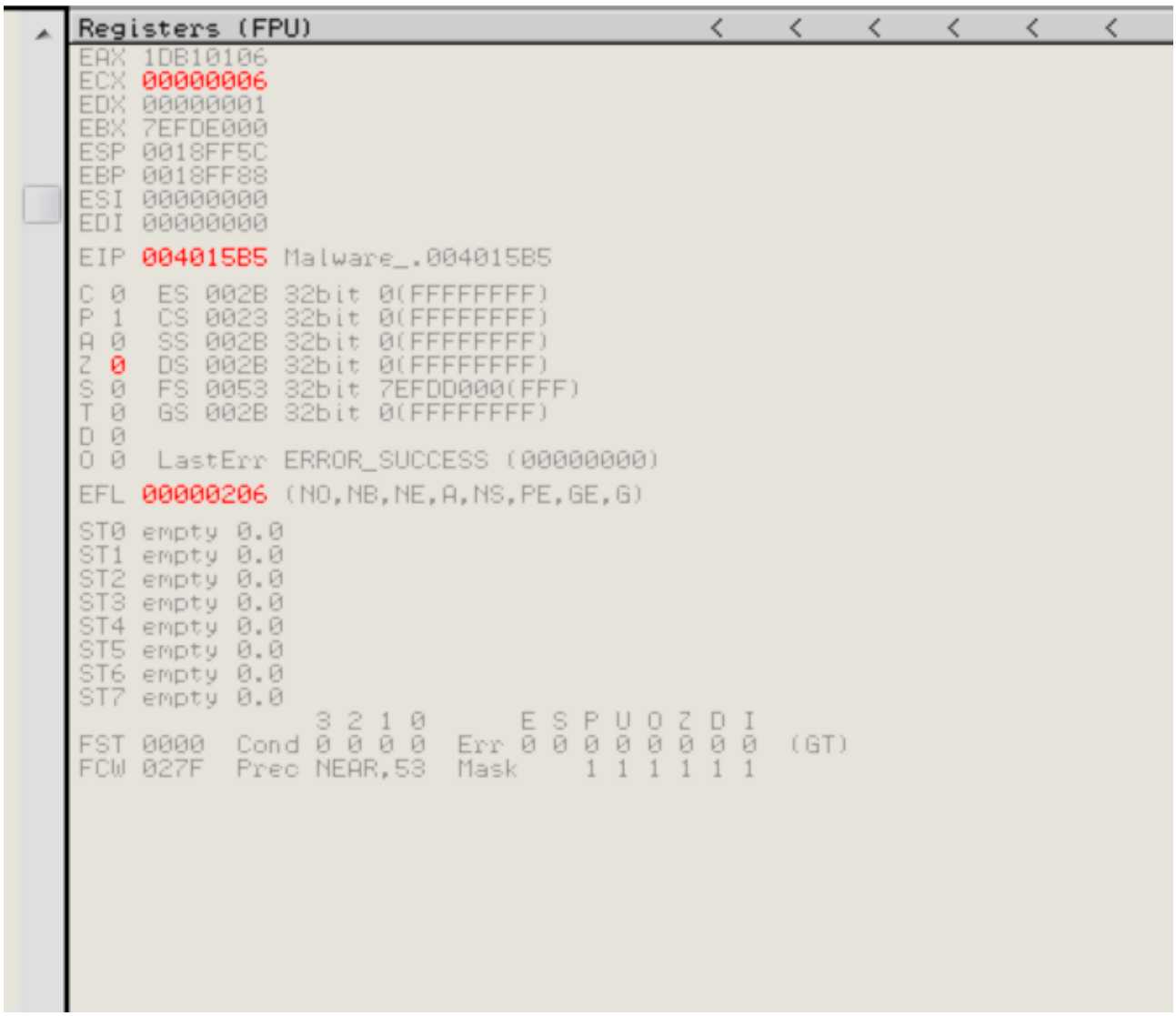


Viene modificato in 0 in quanto si utilizza l'operatore logico xor che inserisce come valore risultante 1 solo e soltanto se i due valori sono discordi e 0 se sono uguali. Dato che fa lo xor con se stesso il risultanto è sempre 0 andando cosi a resettare il valore a 0.

Nel indirizzo 004015AF troviamo invece questo valore di ecx



E, vediamo facendo lo step-into che si modifica in



questo in quanto viene eseguita l'operazione end tra i due operatori e il risultante è 6.

a grandi linee questo malware si insinua nel registro di sistema e atraverso un socket client si collega ad un server da cui scarica virus e li va ad attivare sul computer vittima