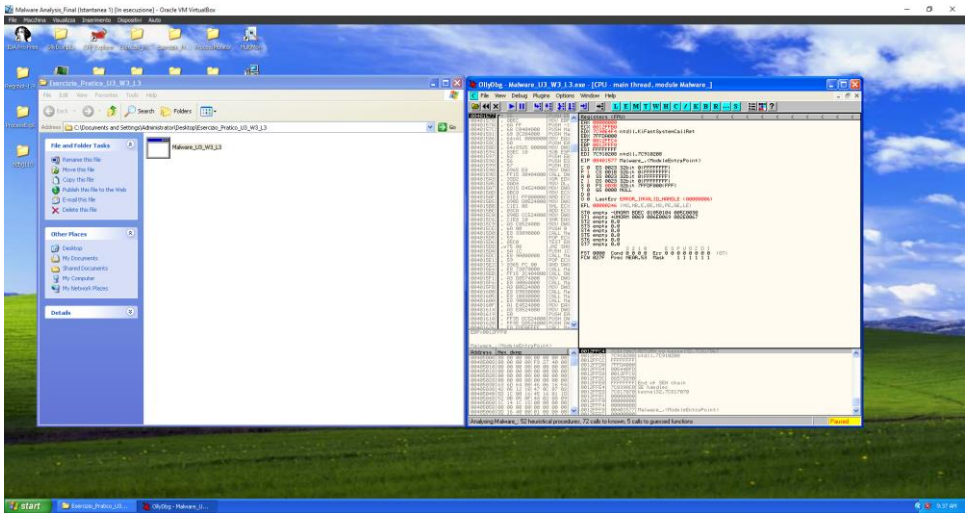
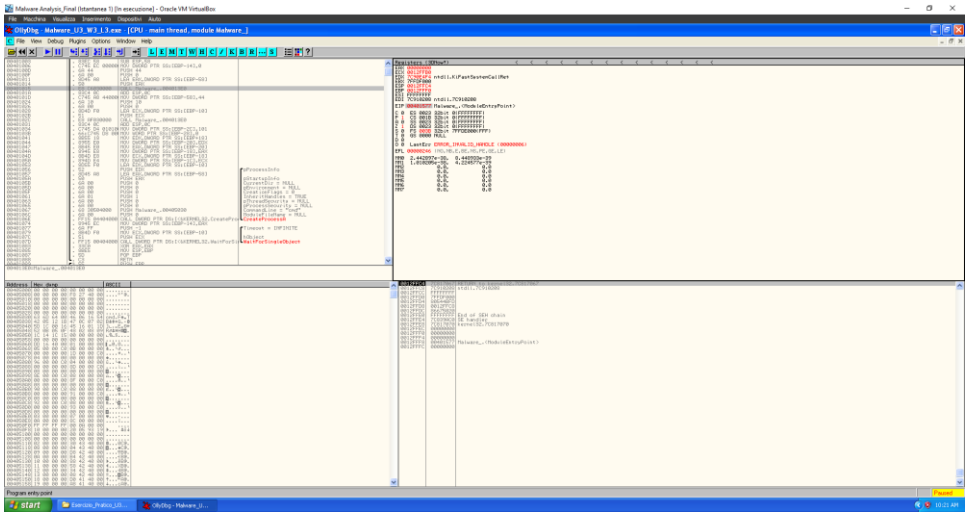
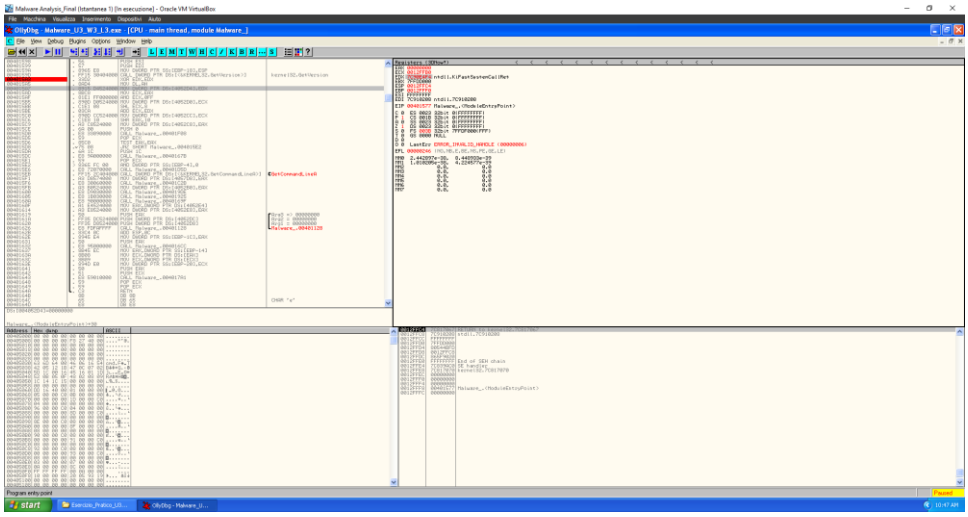


Avvio Malware

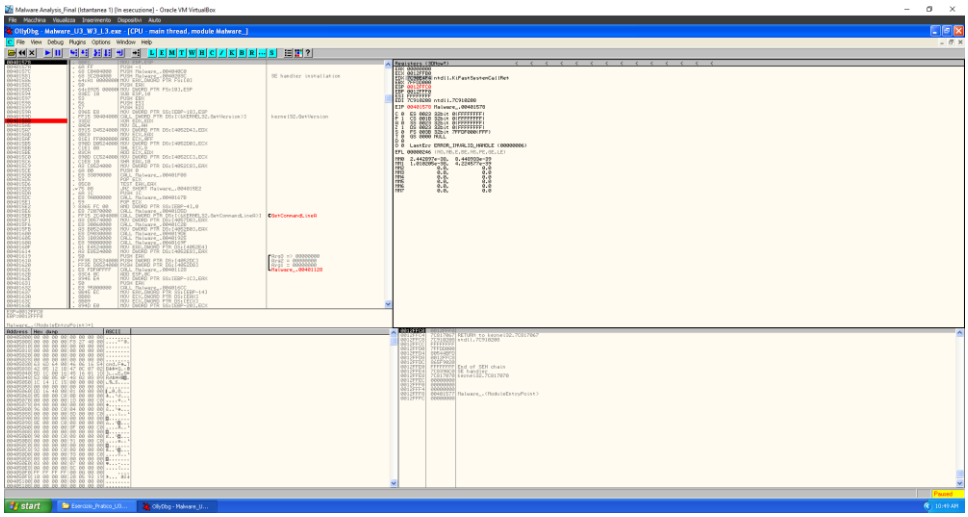


Lo “stack” qui nelle foto chiama una funzione PUSH Malware la prima parte dello “stack(1)” al centro e poi di nuovo 0 come Push, la funzione CreateProcessA indica che il virus sta svolgendo azioni con i processi, ovvero il malintenzionato potrebbe sfruttare ciò per impersonare un utente attraverso la creazioni di processi.

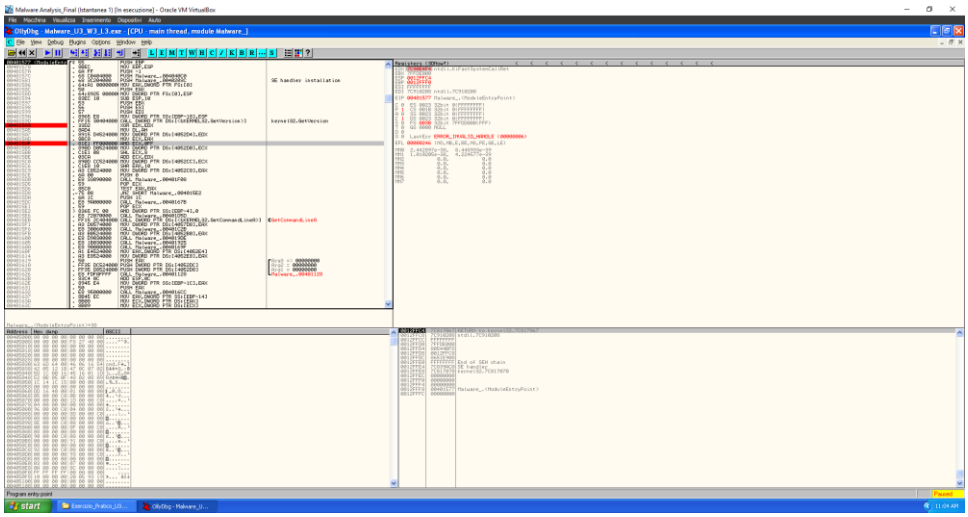


Il valore era di EDX di 8, il malware sta facendo chiamate per avere un comando attraverso le dword.

Valore sopra con ***"Breakpoint"***



Il valore di EDX aggiornato L'istruzione seguita dalle foto è un Mov dai registri ovvero un copia , ha cercato di copiare qualcosa il malware.



Il valore iniziale di ECX è 8 dopo aver trovato la funzione diventa 18

L'istruzione eseguita è Pop ECX