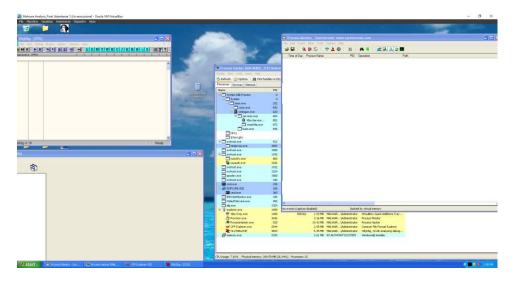
IL Virus calcolatrice qui in basso

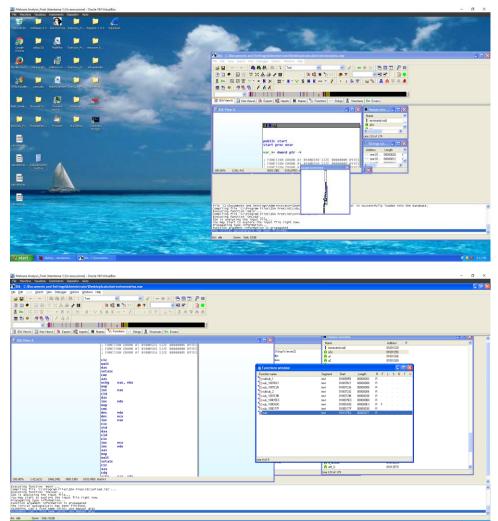


Inizio scansioni in giù



Dalle scansioni si può notare che il virus chiama alcune funzioni, tra cui carica librerie e opre le key di sistema, il virus sfrutta queste funzioni per accedere tramite registro alle informazioni di sistema.

Usando IDA PRO



Si possono vedere alcuni movimenti strani che esso fa il percorso per esempio e alcune funzioni che esso ha implementato, quella in particolare che la ha rilevata anche ollydbg, ovvero quella dei registri nell'ultima foto.

Il virus potrebbe essere un worm tranquillamente, per il fatto che gira molti registri e per il fatto che appena aperto esso usi anche altri file eseguibili,che potrebbero essere le funzioni o altro che olui usa.