

Các API sử dụng

Sử dụng LoadLibraryA() và GetProcAddress() để khôi phục IAT

Ngoài ra packer còn sử dụng

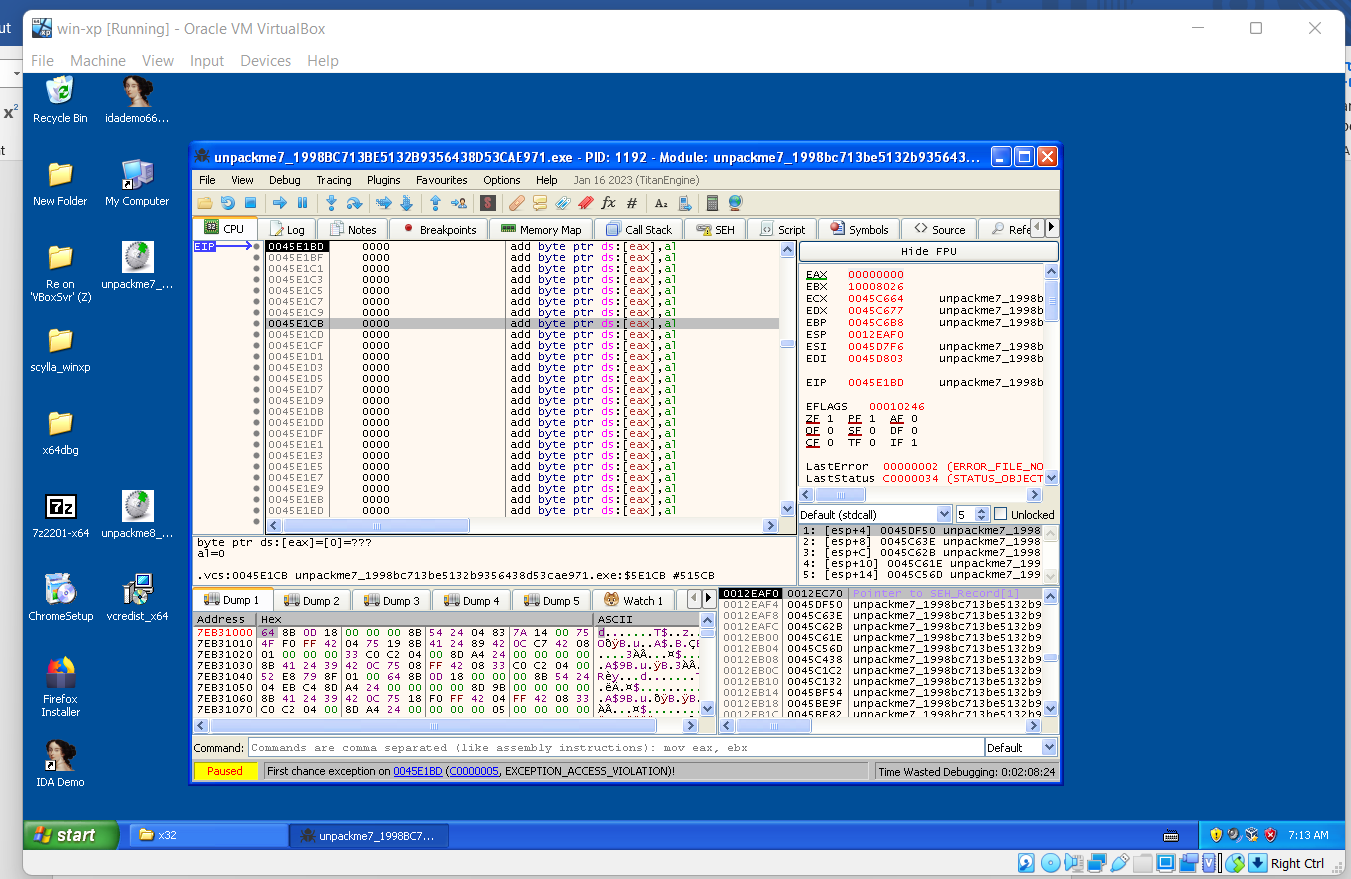
Các kĩ thuật Anti debug : IsDebuggerPresent(), BlockInput(), kiểm tra tên process con ( dùng Create32SnapShot từ đó truy suất thông tin tiến trình )

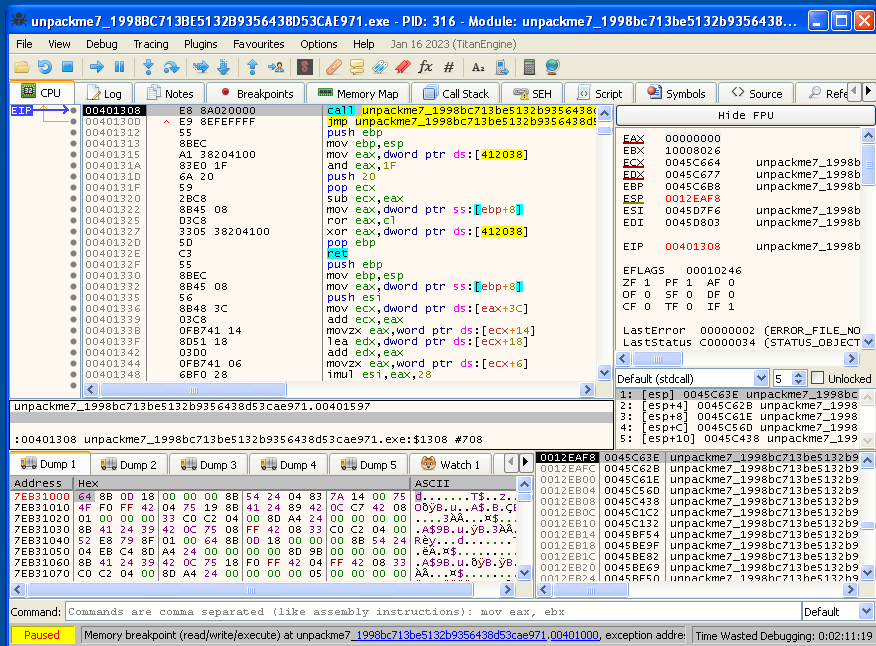
Tạo các đoạn mã giả gây khó khăn khi phân tích file

Chương trình chỉ chạy trên winxp

Thực thi chương trình tới đây (F9 1 lẫn nữa chương trình sẽ thực thi hoàn toàn)

Load lại chương trình và chạy tới đây đặt breakpoint on accsess  vào section text





Dùng scylla dump ra và load file vào IDA ta xác định được winmain

