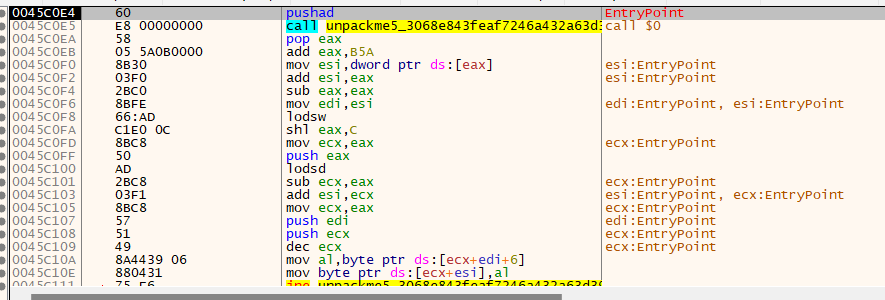


Load file vào x64dbg



1. File sẽ thực thi phần tại phần code đã được thêm vào
2. Lưu lại trạng thái của các thanh ghi hiện tại bằng pushad
3. Giải nén phần code thực thi ban đầu

* Dựa vào thuật toán nén để khôi phục ngoài các câu lệnh cơ bản còn sử dụng các API
* GetModuleHandleA
* GetProcAddress
* Từ 2 hàm trên lấy được con trỏ hàm của **VirtualProtect** : thay đổi quyền truy cập ( hàm này sử dụng sau để đảm bảo code sau khi khôi phục sẽ được bảo vệ)

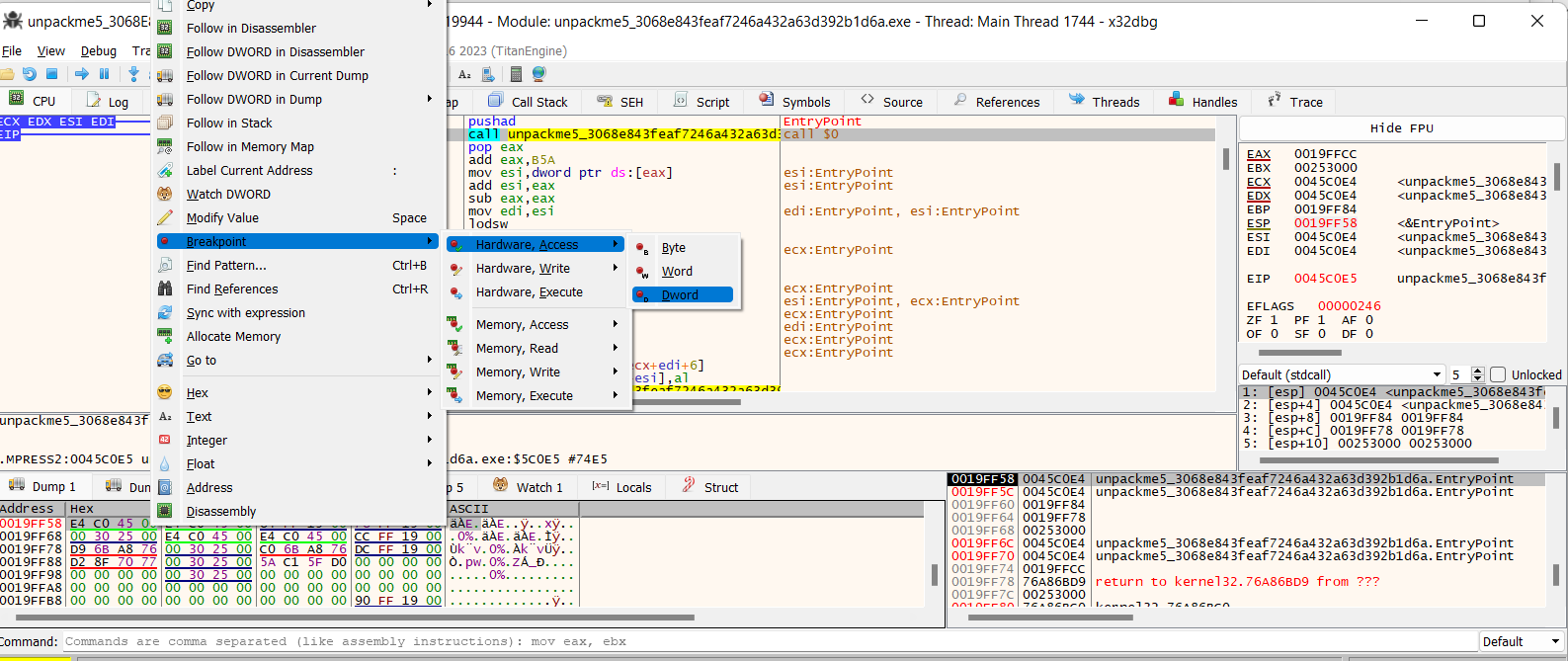
1. Khôi phục lại IAT

* GetModuleHandleA
* GetProcAddress

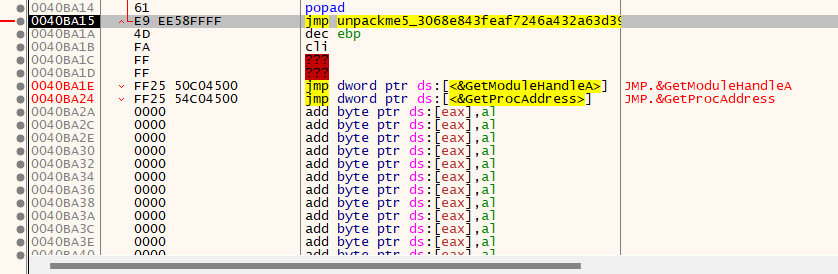
1. Khôi phục lại trạng thái thanh ghi bằng popad
2. Jump tới OEP gốc của file thực thi ban đầu

Nhận thấy chương trình có pushad => dấu hiệu để tìm OEP

Set breakpoint on access



F9 để nhảy đến câu lệnh popad. Chương trĩnh dẫn tới 1 câu lệnh jmp



Nhảy vào đây ta tìm được oep

