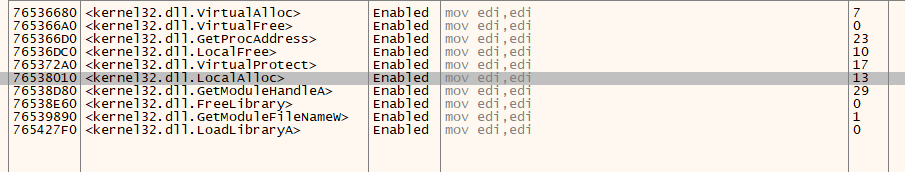
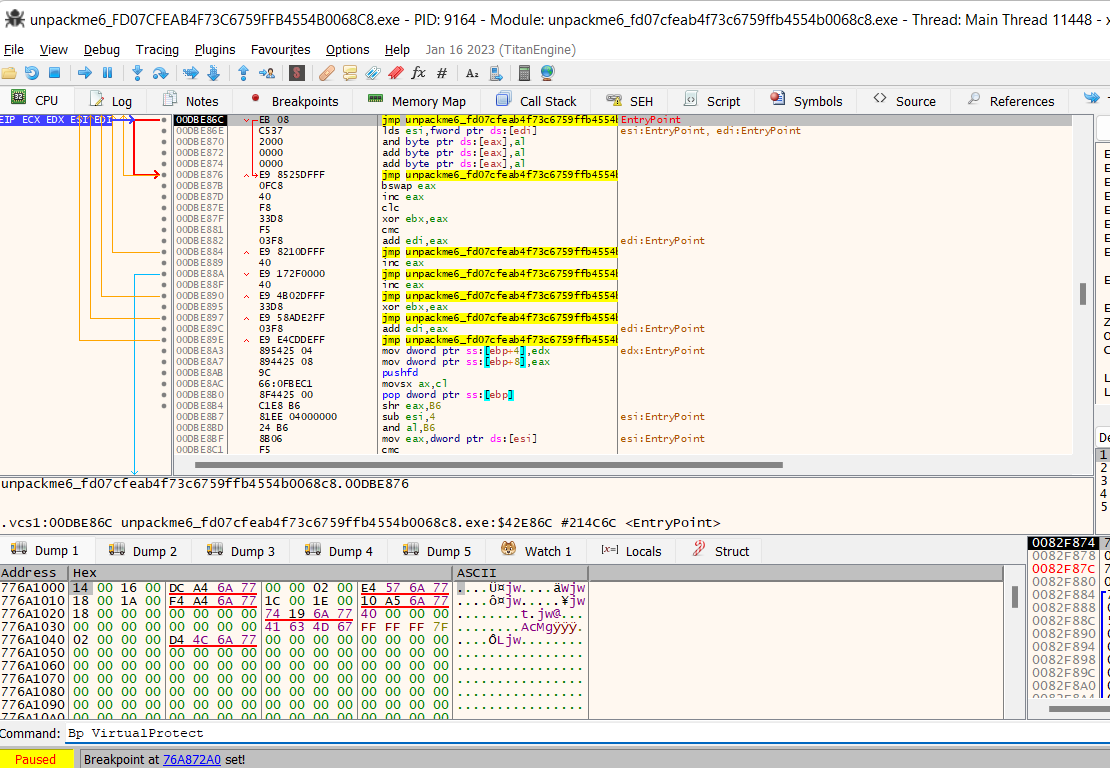


Đây là các API mà chương trình sử dụng để khôi phục code thực thi gốc và IAT

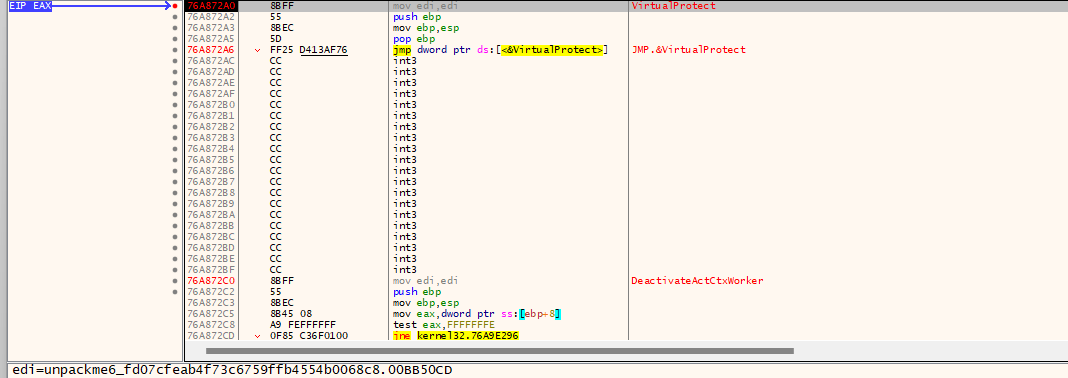


Packer này ko sử dụng pushad như những packer trước nên ko thể lần theo phương pháp cũ để tìm OEP. Phải dựa vào các API mà packer sử dụng lúc khôi phục code để tìm code thực thi gốc.

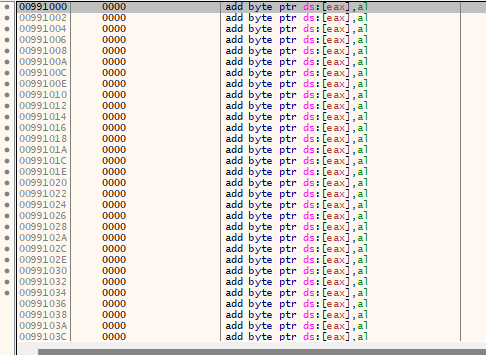
Set break point tại VirtualProtect



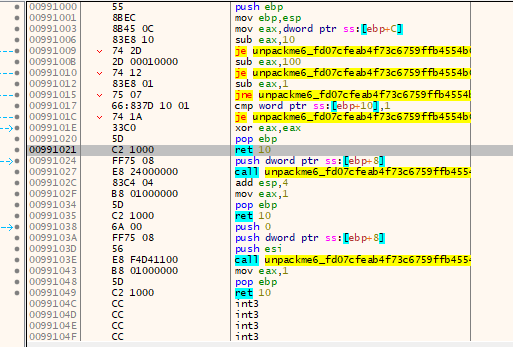
F9 nhảy tới VirtualProtect



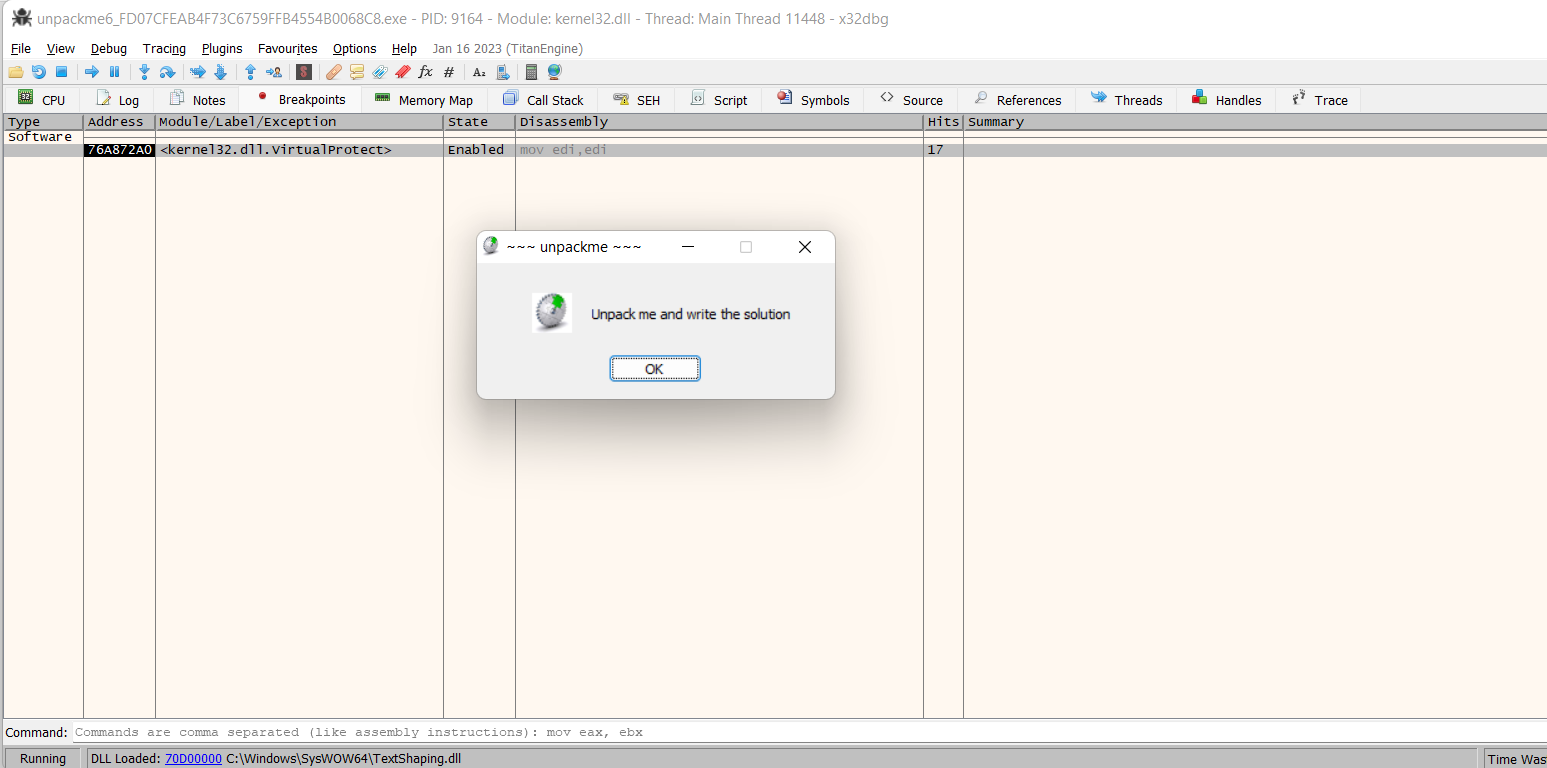
Ban đầu trong .text chưa có code



Sau khi F9 vài lần ta có code trong .text chứng tỏ chương trình đang khôi phục lại code thực thi ban đầu

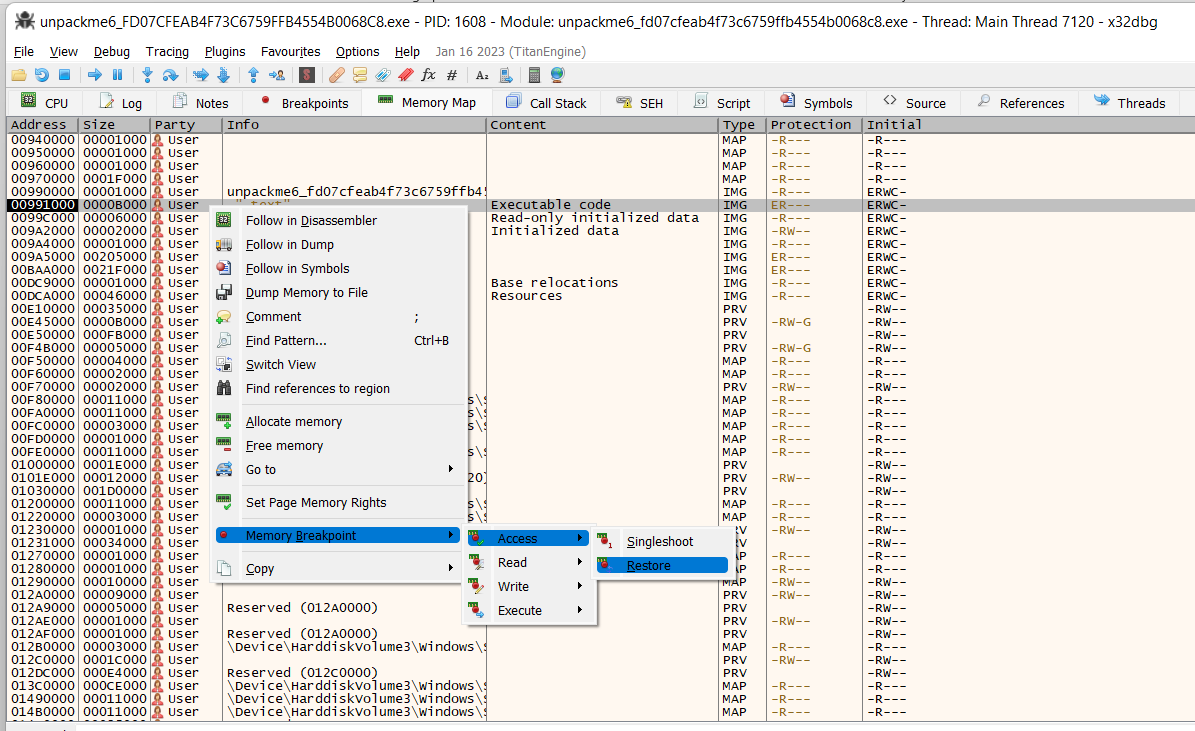


Tiếp tục F9 sau 17 hit thì F9 1 lần nữa chương trình đã thực thi

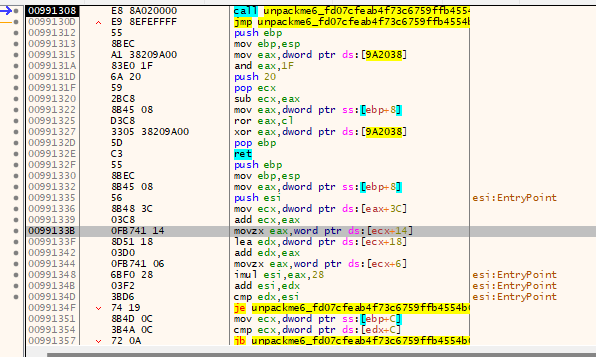


Load lại chương trình và làm tương tự trên nhưng ta dừng khi VirtualProtect được gọi 17 lần

Mục đích là vì lúc đầu ta test thử thì xác định hàm VirtualProtect được gọi tối đa 17 lần lúc này code thực thi mới được khôi phục hoàn toàn và sau khi code thực thi khôi phục hoàn toàn ta mới có thể tìm được OEP gốc của chương trình



Set memory break point access sau đó F9 ta sẽ nhảy tới OEP



IDA đã xác định được WinMain

