

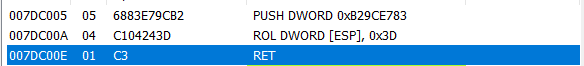
1. File sẽ thực thi phần tại phần code đã được thêm vào
2. Lưu lại trạng thái của các thanh ghi hiện tại bằng pushad
3. Giải nén phần code thực thi ban đầu

* 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 3 con trỏ hàm của
  + - * + VirtualAlloc : cấp phát bộ nhớ ảo
        + VirtualFree : giải phóng
        + 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

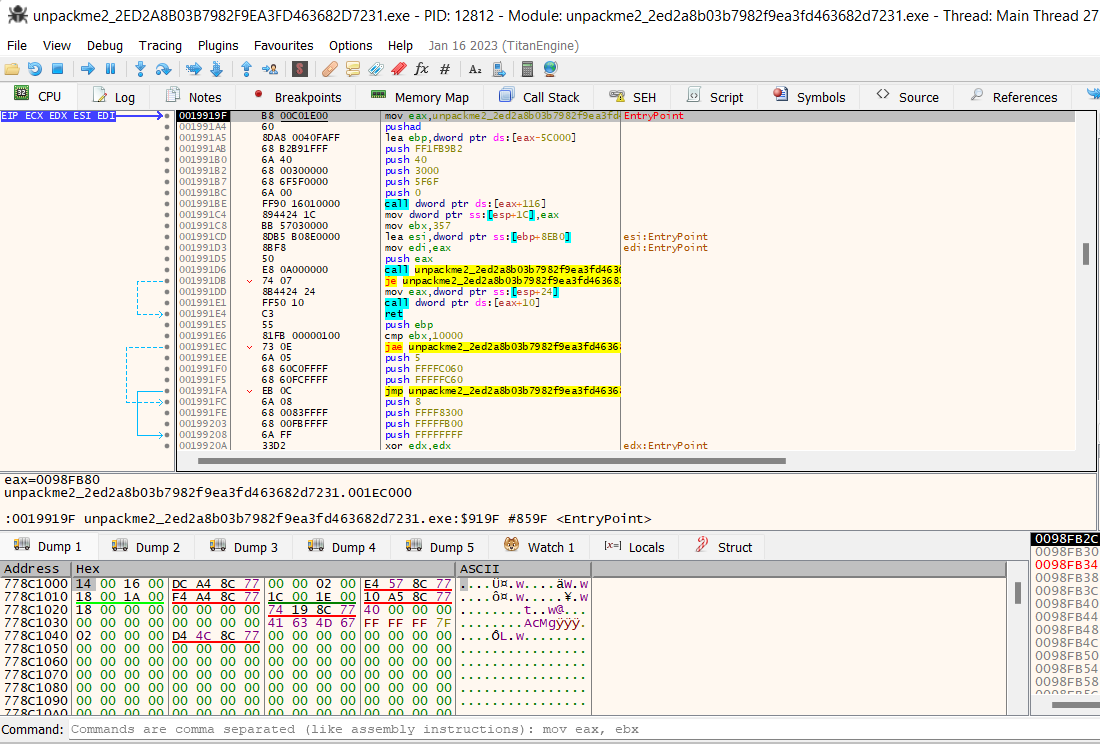
* GetModuleHandleA
* GetProcAddress

Có 1 số hàm API không được gọi trực tiếp mà gọi bằng lệnh ret (đẩy giá trị vào đỉnh ngay xếp xong ret)



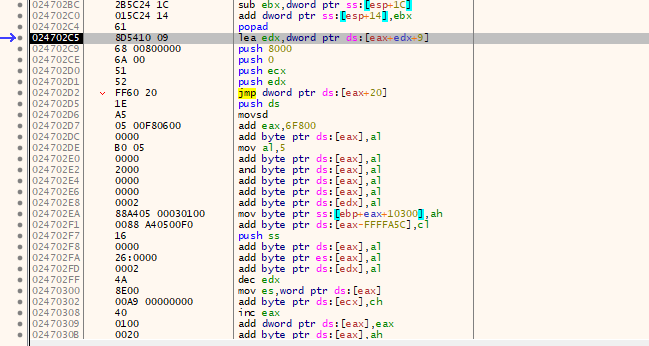
1. Khôi phục lại trạng thái thanh ghi bằng popad
2. Jump tới OEP gốc của file thực thi ban đầu

Load file vào x64 f9 để nhảy tới entry point



Nhận thấy có pushad. Ta đặt memory break point on access tại esp

F9 chương trình nhảy tới đây



Tiếp tục trace theo chương trình tới được OEP của chương trình

