Sinh viên: Bùi Xuân Thái 18521379

Giảng viên hướng dẫn: PhD. Nguyễn Ngọc Tự

DLL INJECTION (MEMORY ACCESS CONTROL ATTACKS)

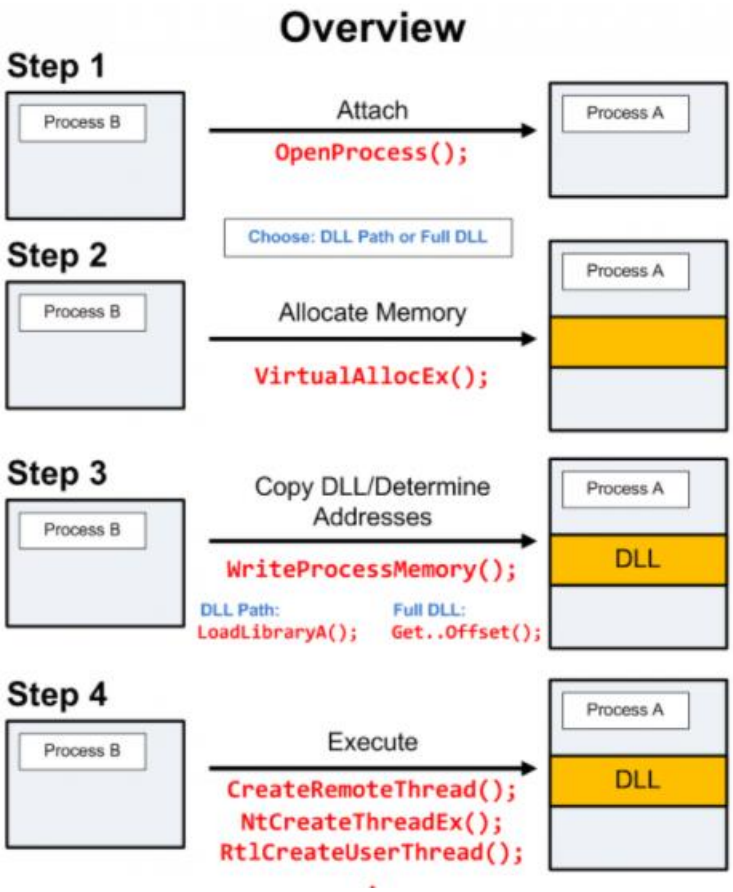
1. Định nghĩa

- DLL Injection là quá trình chèn code vòa một tiến trình (process) đang chạy. Code được sử dụng ở đây là dạng thư viện liên kết động (DLL). Tuy nhiên không phải chỉ chèn được code dạng DLL, chúng ta có thể chèn code ở nhiều dạng khác như exe, handwritten,…. Điều quan trọng là chúng ta có đủ quyền hệ thống để thao tác với tiến trình của ứng dụng khác hay không.

2. Phương thức hoạt động, phân tích các nguy cơ

* Phương thức hoạt động;

- Windows API đã cung cấp cho chúng ta một vài các hàm để can thiệp và thao tác vào những chương trình khác cho mục đích Debug. Chúng ta tận dụng các API này để thực hiện chèn DLL. Quá trình chèn DLL Injection gồm 4 bước:



+ B1: Can thiệp vào process

+ B2: Cấp phát một vùng nhớ trong process

+ B3: Copy toàn bộ DLL hoặc đường dẫn DLL vào vùng nhớ đó và xác định vị trí của vùng nhớ

+ B4: Process thực thi DLL

* Các nguy cơ

- Các mã được tiêm vào có thể móc vào các lời gọi hàm hệ thống, đọc nội dung các văn bản mật khẩu, văn bản quan trọng

- Hack các game online bằng cách chèn code DLL vào file .exe của game đó.

Ví dụ: Game Among Us hack được ta luôn luôn là sát thủ,….

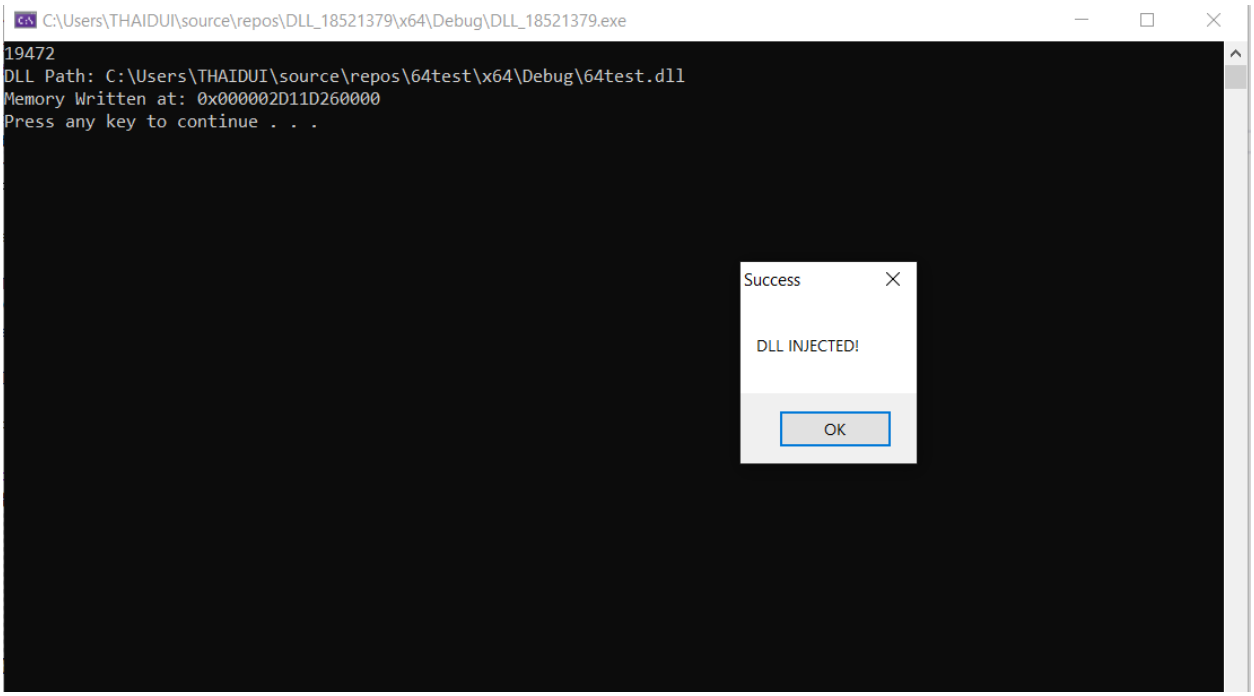
Tuy nhiên, hầu hết các game đều có hệ thống tự bảo vệ chính mình khỏi DLL Injection

3. Phương pháp thực hiện

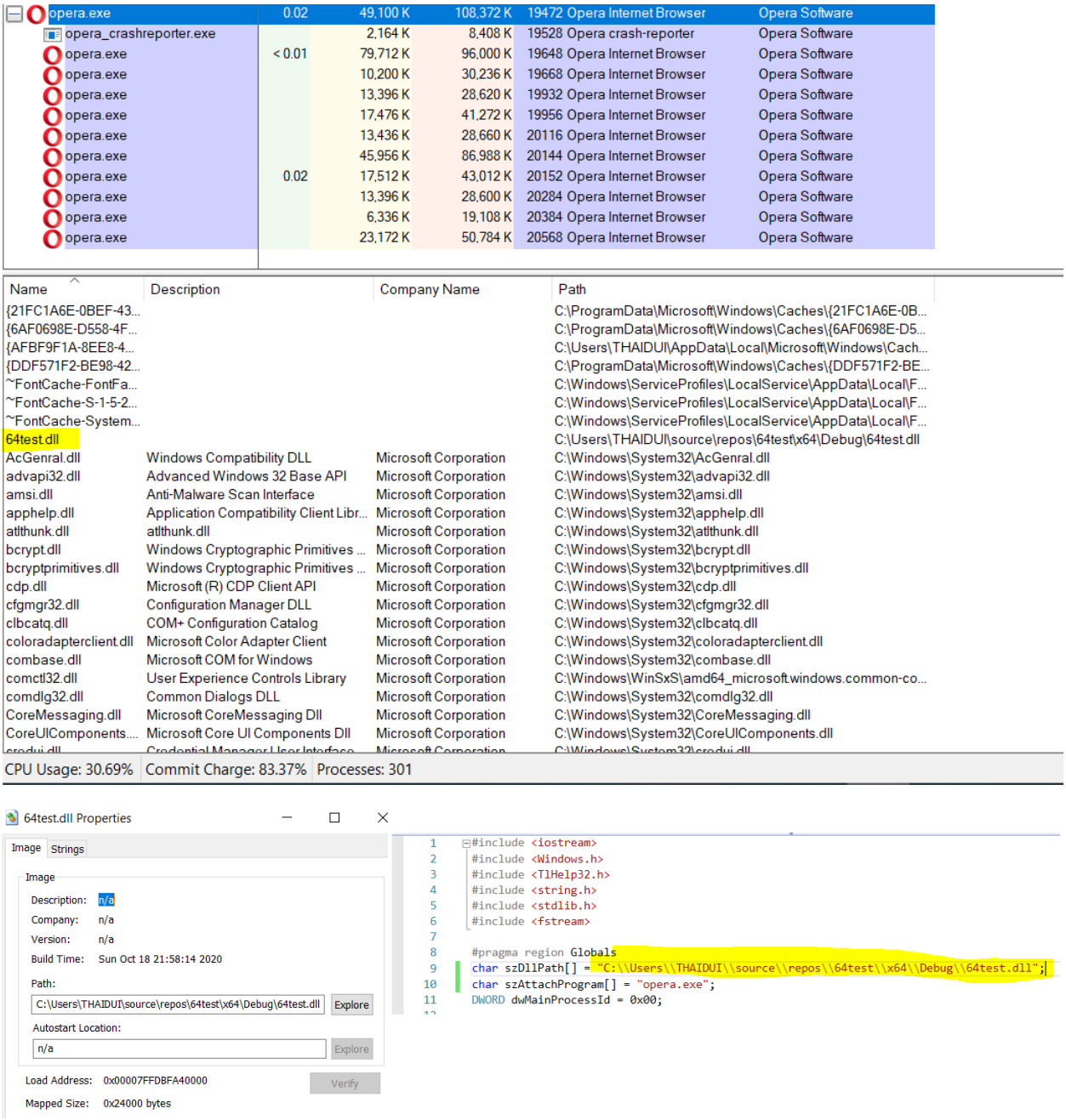
- Video demo: https://drive.google.com/drive/folders/1VPzvsiVfpUQodung-PTBRLo05ivpUsws

- Ảnh chụp màn hình

Chạy code với path dll là: C:\Users\THAIDUI\source\repos\64test\x64\Debug\64test.dll



Dùng Process Explorer xem tiến trình opera.exe, ta thấy có file 64test.dll xuất hiện trong tiến trình, ta đã chèn thành công.



4. Đề xuất cách phòng chống

- Có nhiều cách để phát hiện ra kỹ thuật DLL Injection, nhưng cách phổ biến là kiểm tra danh sách các module import và tìm các vùng nhớ có quyền đọc ghi của process