

Sinh viên: Bùi Xuân Thái      18521379

Giảng viên hướng dẫn: PhD. Nguyễn Ngọc Tự

# **DLL INJECTION (MEMORY ACCESS CONTROL ATTACKS)**

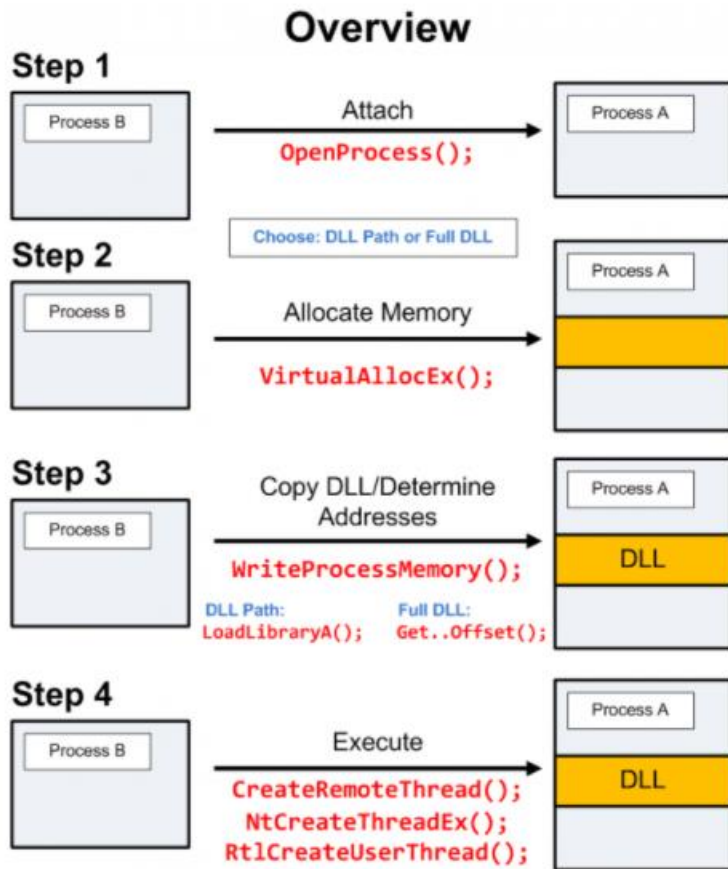
## **1. Định nghĩa**

- DLL Injection là quá trình chèn code vào 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

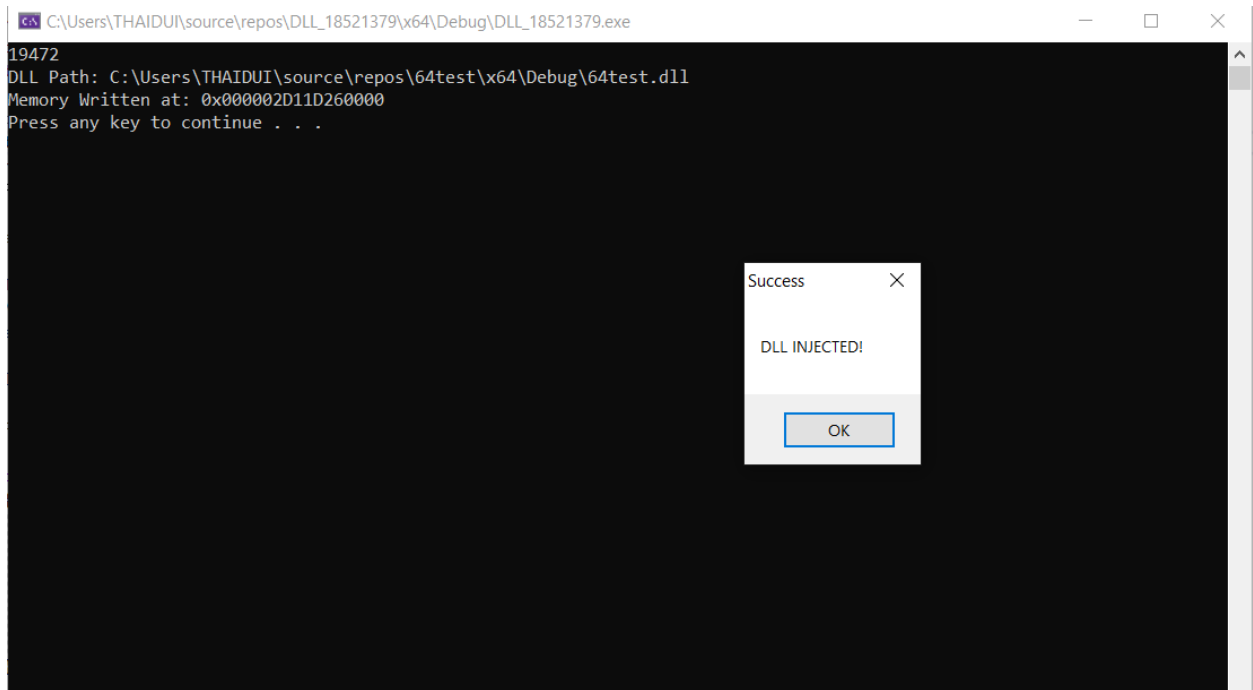
### 3. Phương pháp thực hiện

- Video demo: <https://drive.google.com/drive/folders/1VPzvsiVfpUQodung-PTBRL05ivpUsws>

- 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.

opera.exe	0.02	49,100 K	108,372 K	19472	Opera Internet Browser	Opera Software
opera_crashreporter.exe		2,164 K	8,408 K	19528	Opera crash-reporter	Opera Software
opera.exe	< 0.01	79,712 K	96,000 K	19648	Opera Internet Browser	Opera Software
opera.exe		10,200 K	30,236 K	19668	Opera Internet Browser	Opera Software
opera.exe		13,396 K	28,620 K	19932	Opera Internet Browser	Opera Software
opera.exe		17,476 K	41,272 K	19956	Opera Internet Browser	Opera Software
opera.exe		13,436 K	28,660 K	20116	Opera Internet Browser	Opera Software
opera.exe		45,956 K	86,988 K	20144	Opera Internet Browser	Opera Software
opera.exe	0.02	17,512 K	43,012 K	20152	Opera Internet Browser	Opera Software
opera.exe		13,396 K	28,600 K	20284	Opera Internet Browser	Opera Software
opera.exe		6,336 K	19,108 K	20384	Opera Internet Browser	Opera Software
opera.exe		23,172 K	50,784 K	20568	Opera Internet Browser	Opera Software

Name	Description	Company Name	Path
{21FC1A6E-0BEF-43...			C:\ProgramData\Microsoft\Windows\Caches\{21FC1A6E-0B...
{6AF0698E-D558-4F...			C:\ProgramData\Microsoft\Windows\Caches\{6AF0698E-D5...
{AFBF9F1A-8EE8-4...			C:\Users\THAIDUI\AppData\Local\Microsoft\Windows\Cach...
{DDF571F2-BE98-42...			C:\ProgramData\Microsoft\Windows\Caches\{DDF571F2-BE...
~FontCache-FontFa...			C:\Windows\ServiceProfiles\LocalService\AppData\Local\F...
~FontCache-S-1-5-2...			C:\Windows\ServiceProfiles\LocalService\AppData\Local\F...
~FontCache-System...			C:\Windows\ServiceProfiles\LocalService\AppData\Local\F...
64test.dll			C:\Users\THAIDUI\source\repos\64test\x64\Debug\64test.dll
AcGenral.dll	Windows Compatibility DLL	Microsoft Corporation	C:\Windows\System32\AcGenral.dll
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\System32\advapi32.dll
amsi.dll	Anti-Malware Scan Interface	Microsoft Corporation	C:\Windows\System32\amsi.dll
apphelp.dll	Application Compatibility Client Libr...	Microsoft Corporation	C:\Windows\System32\apphelp.dll
atthunk.dll	atthunk.dll	Microsoft Corporation	C:\Windows\System32\atthunk.dll
bcrypt.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcrypt.dll
bcryptprimitives.dll	Windows Cryptographic Primitives ...	Microsoft Corporation	C:\Windows\System32\bcryptprimitives.dll
cdp.dll	Microsoft (R) CDP Client API	Microsoft Corporation	C:\Windows\System32\cdp.dll
cfgmgr32.dll	Configuration Manager DLL	Microsoft Corporation	C:\Windows\System32\cfgmgr32.dll
clbcatq.dll	COM+ Configuration Catalog	Microsoft Corporation	C:\Windows\System32\clbcatq.dll
coloradapterclient.dll	Microsoft Color Adapter Client	Microsoft Corporation	C:\Windows\System32\coloradapterclient.dll
combase.dll	Microsoft COM for Windows	Microsoft Corporation	C:\Windows\System32\combase.dll
comctl32.dll	User Experience Controls Library	Microsoft Corporation	C:\Windows\WinSxS\amd64_microsoft-windows.common-co...
comdlg32.dll	Common Dialogs DLL	Microsoft Corporation	C:\Windows\System32\comdlg32.dll
CoreMessaging.dll	Microsoft CoreMessaging Dll	Microsoft Corporation	C:\Windows\System32\CoreMessaging.dll
CoreUIComponents...	Microsoft Core UI Components Dll	Microsoft Corporation	C:\Windows\System32\CoreUIComponents.dll
credui.dll	Credential Manager User Interface	Microsoft Corporation	C:\Windows\System32\credui.dll

CPU Usage: 30.69% Commit Charge: 83.37% Processes: 301

64test.dll Properties

Image
Strings

Image

Description: n/a
Company: n/a
Version: n/a
Build Time: Sun Oct 18 21:58:14 2020
Path: C:\Users\THAIDUI\source\repos\64test\x64\Debug\64test.dll
Autostart Location: n/a
Load Address: 0x00007FFD8FA40000
Mapped Size: 0x24000 bytes

```

1  #include <iostream>
2  #include <Windows.h>
3  #include <TlHelp32.h>
4  #include <string.h>
5  #include <stdlib.h>
6  #include <fstream>
7
8  #pragma region Globals
9  char szDllPath[] = "C:\\Users\\THAIDUI\\source\\repos\\64test\\x64\\Debug\\64test.dll";
10 char szAttachProgram[] = "opera.exe";
11 DWORD dwMainProcessId = 0x00;

```

## 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