1. CLASSIC DLL INJECTION

Tool: Dll injector

Nguồn tải: https://github.com/hasherezade/dll\_injector/tree/master

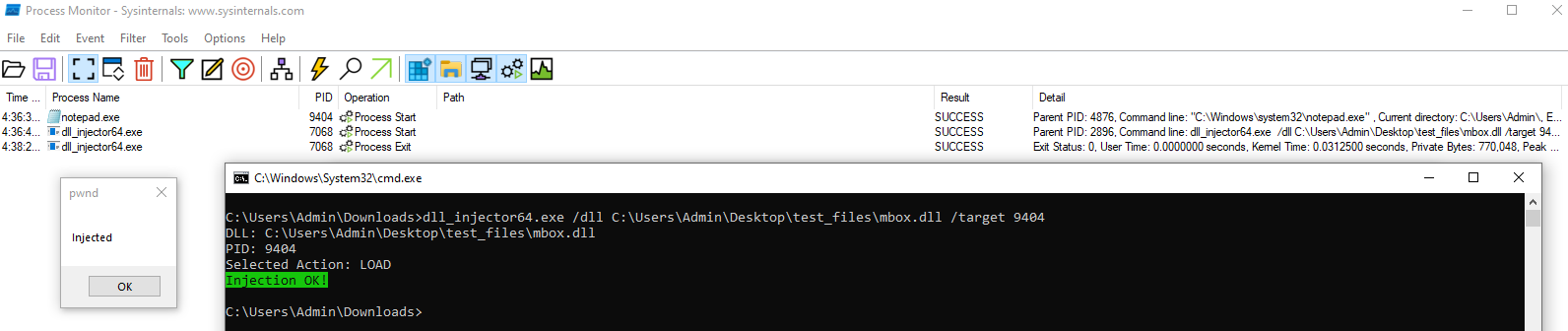
Dll injector hỗ trợ inject code vào process trong 2 trường hợp

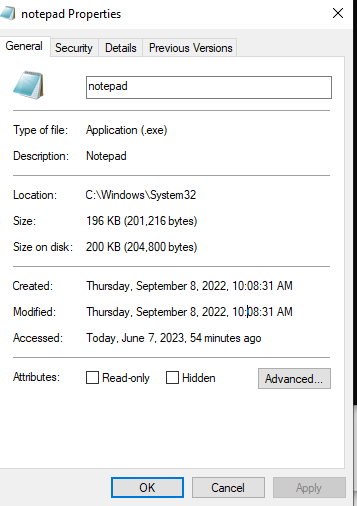
* Tiên trình đích đã được khởi chạy

Để inject 1 file dll vào tiến trình đã được khởi chạy cần có 2 tham số

Tham số thứ nhất là đường dẫn tới file dll muốn inject vào process

Tham số thứ 2 là PID (Process identifier) của tiến trình đích



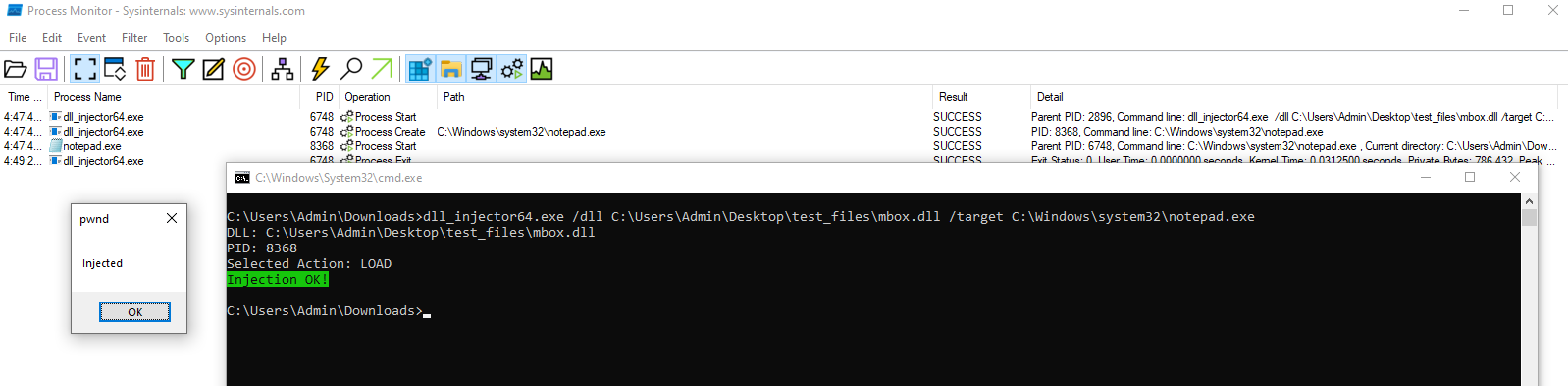


Sau khi kết thúc tiến trình trên, truy suất thông tin của file notepad.exe ta thấy file này hoàn toàn không bị chỉnh sửa.

* Tiến trình đích chưa khởi chạy

Tham số thứ nhất là đường dẫn tới file dll

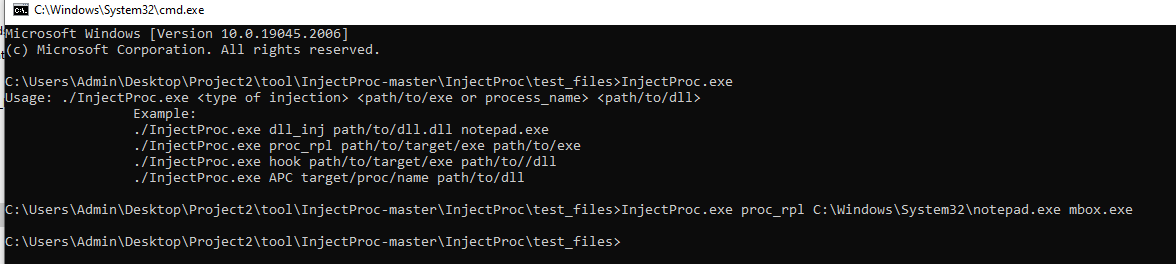
Tham số thứ 2 là đường dẫn tới file thực thi



1. PORTABLE EXECUTABLE INJECTION (PE INJECTION) ( chưa tìm thấy) nếu cần thiết có thể code
2. Process hollowing ( đã trình bày trong báo cáo lần trước

tool InjectProc : <https://github.com/secrary/InjectProc>

tool này chỉ hỗ trợ các file pe 64



ở đây ta chọn taget process chính là notepad.exe còn mbox.exe là file mà chúng ta muốn chèn vào chương trình notepad.exe

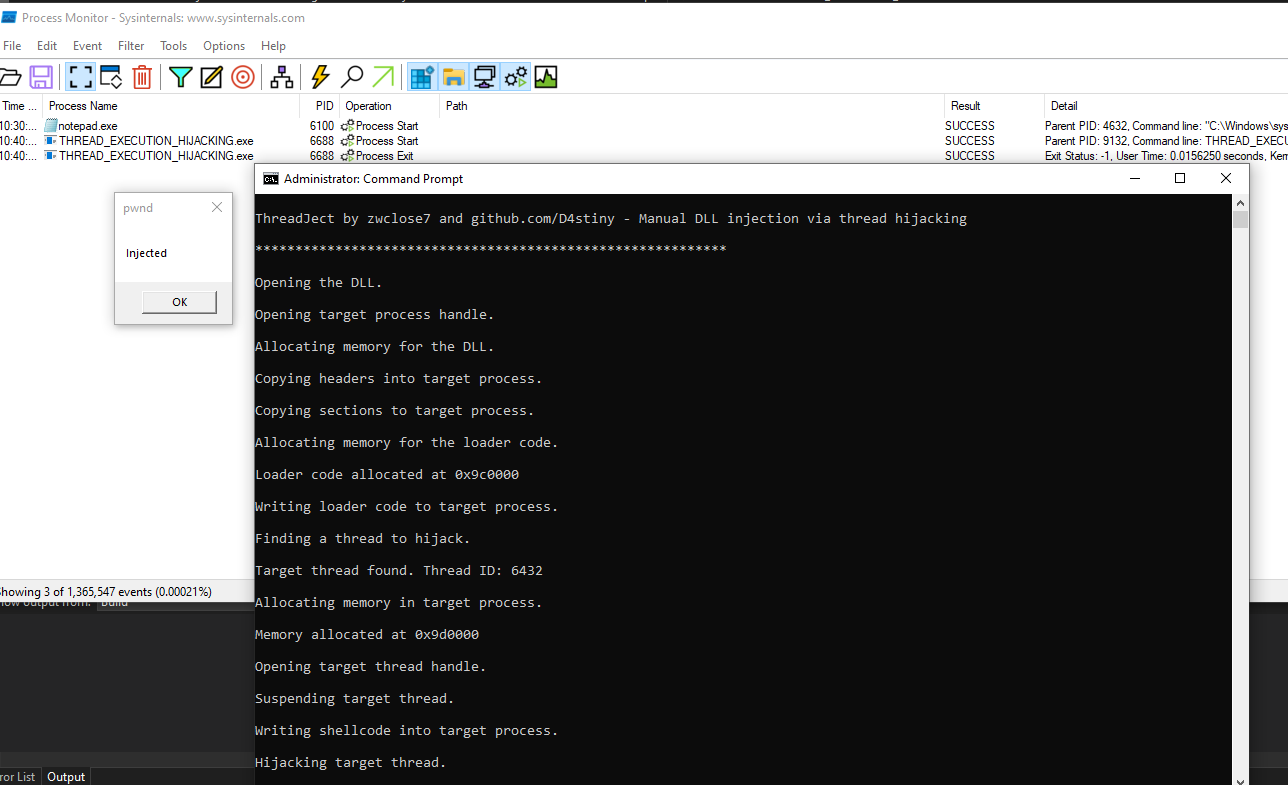
1. THREAD EXECUTION HIJACKING

Tool threadJect :https://github.com/D4stiny/ThreadJect

Để inject 1 file dll vào tiến trình đã được khởi chạy cần có 2 tham số

Tham số thứ nhất là pid của tiến trình đích

Tham số thứ 2 là đường dẫn file DLL



https://github.com/hasherezade/dll\_injector/tree/master

<https://github.com/secrary/InjectProc>

https://github.com/D4stiny/ThreadJect

https://github.com/MahmoudZohdy/Process-Injection-Techniques