Từ việc điều khiển C2 máy nạn nhân, cài driver độc hại và ứng dụng để tương tác với driver đó:  
A screenshot of a computer

Description automatically generated

Chuyển máy nạn nhân sang chế độ thử nghiệm để không bị cảnh báo khi cài driver không chính thức từ Microsoft:

bcdedit /set testsigning on

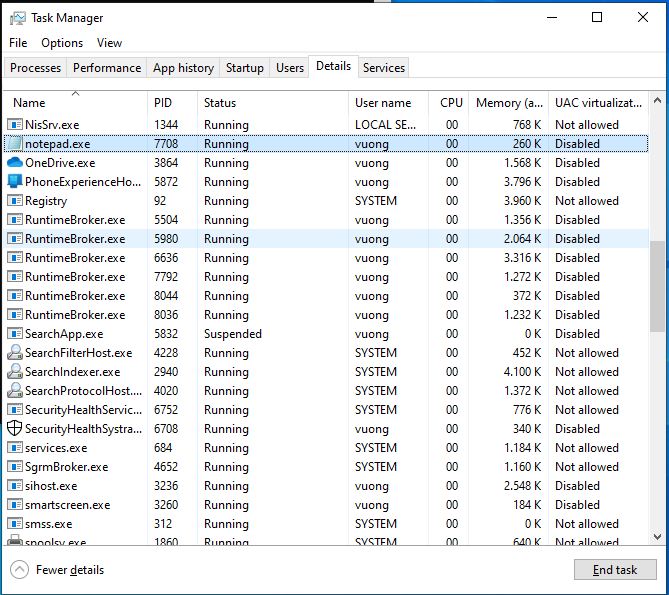
Bắt đầu 1 dịch vụ để chạy driver độc hại:

A screenshot of a computer

Description automatically generated

**Mở notepad và thực hiện demo ẩn tiến trình:**

Tìm kiếm PID các tiến trình đang chạy:



Thực hiện ẩn tiến trình với PID 7708 thông qua ứng dụng để tương tác với driver đã cài:

A screen shot of a computer

Description automatically generated

Tiến trình đã bị ẩn khỏi danh sách tiến trình nhưng ứng dụng vẫn hoạt động:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated