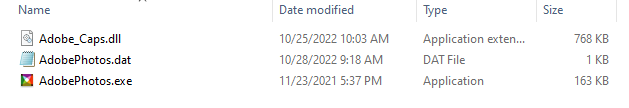
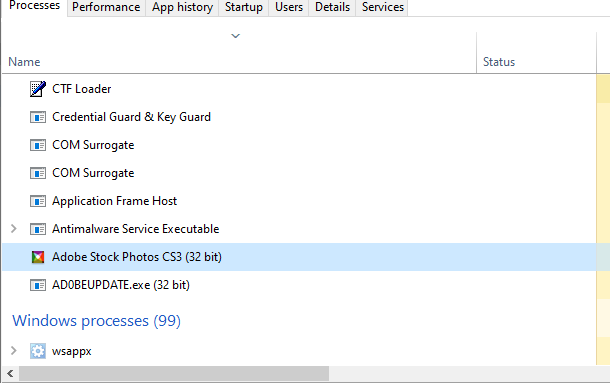


* Thành phần mã độc bung ra

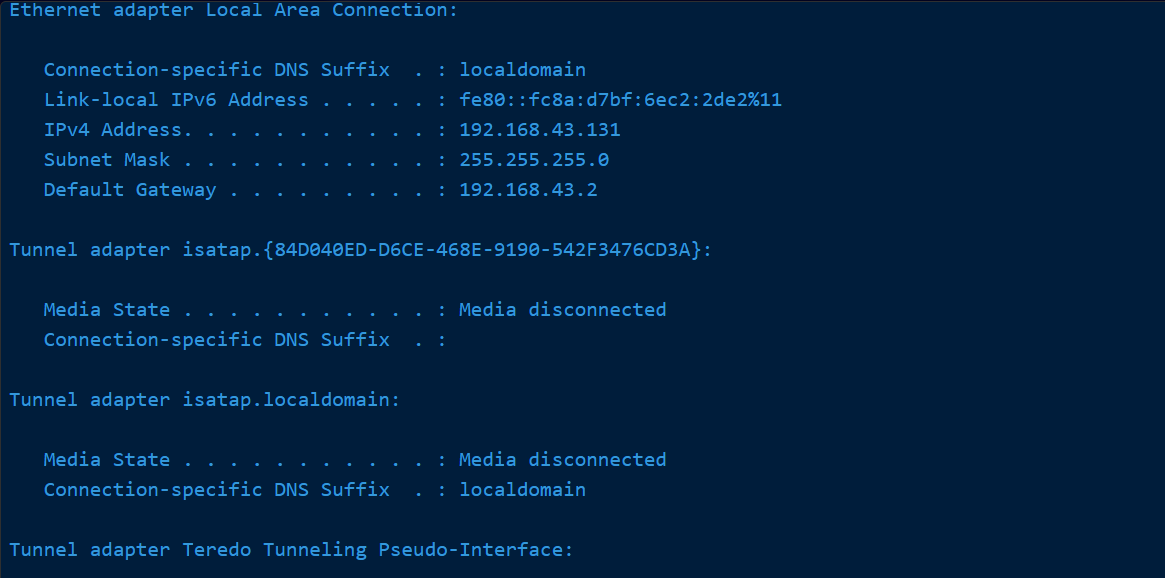


Sau khi triển khai tại máy mục tiêu chiến đấu viên sẽ kích hoạt file thực thi sạch có chữ ký số **AdobePhotos.exe.**

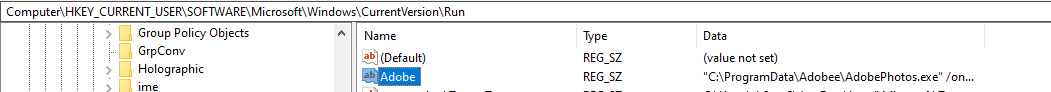
Mục tiêu sẽ được load các payload độc hại từ file DLL đính kèm. Sau khi thực thi sẽ thấy thông tin tiến trình tại Task Manager như sau:



* **Kết nối reveser shell**



* **Tạo duy trì kết nối trên máy mục tiêu**



Sau khi mã độc thực thi trên mục tiêu, việc duy trì kết nối sau khi khởi động máy được thiết lập.