**BÁO CÁO THỰC HÀNH**

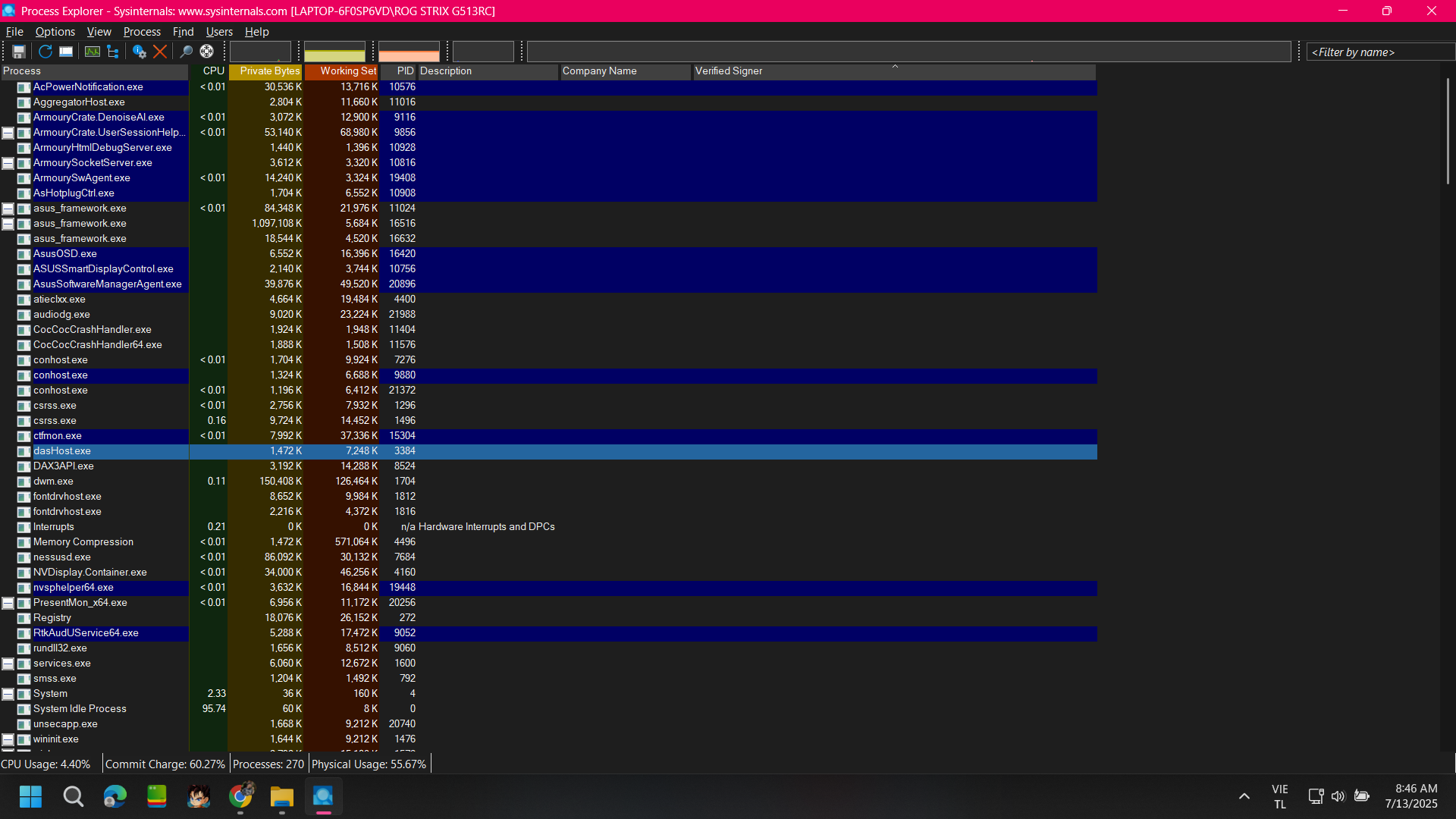
**Laboratory 3 – Malware Detection**

**1. Thông tin sinh viên**

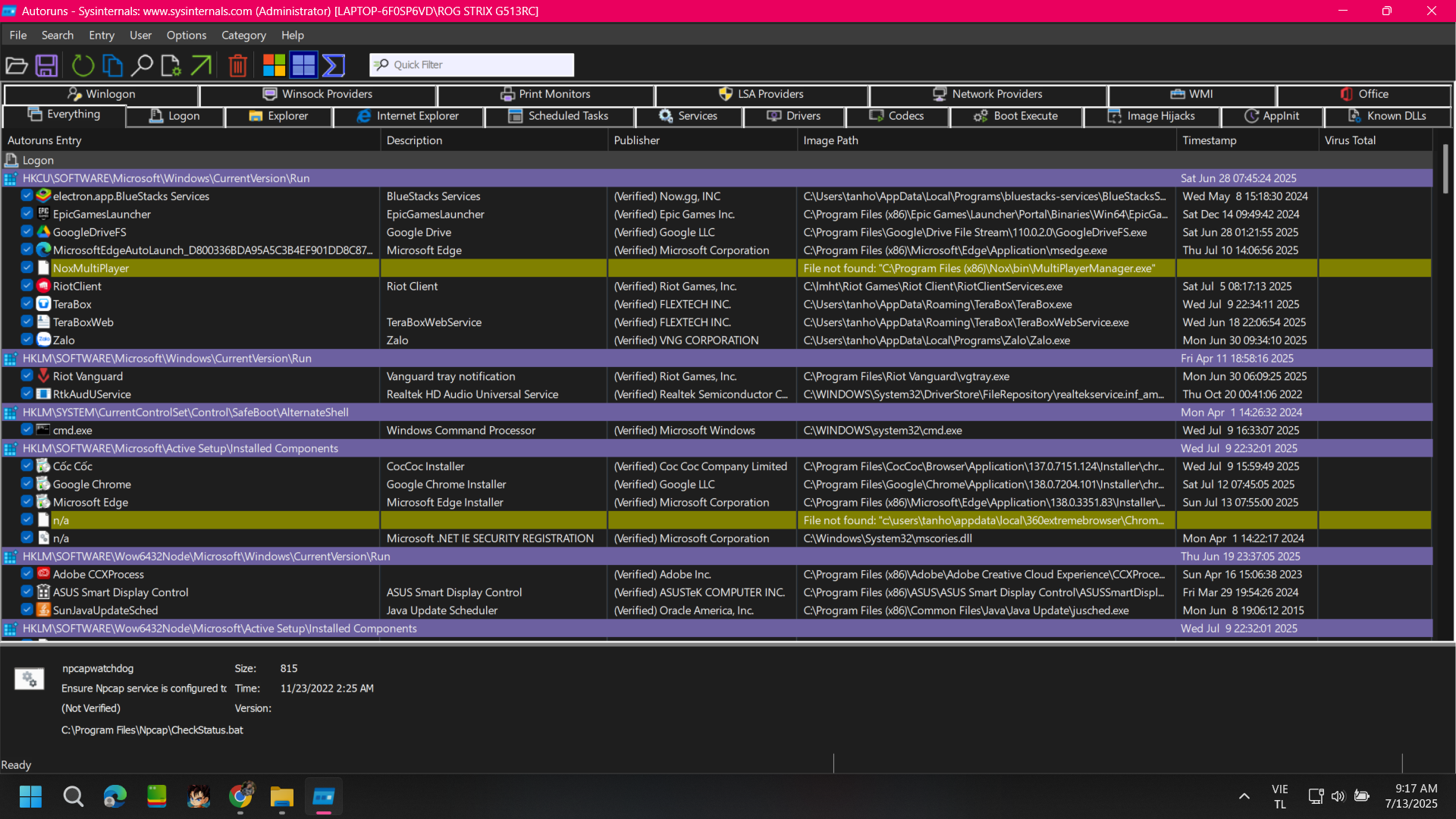
|  |  |  |  |
| --- | --- | --- | --- |
| Họ và tên | MSSV | Lớp | Ngày thực hành |
| Trần Toàn Phát | HTTT2311025 | HTTT2311 | 13/07/2025 |

**2. Mục tiêu bài thực hành**  
- Hiểu được đặc điểm và cơ chế hoạt động của phần mềm độc hại.  
- Sử dụng các công cụ chuyên dụng để phân tích và phát hiện malware.  
- Nhận diện và phân tích các hành vi nghi ngờ thông qua tiến trình, kết nối mạng, registry, và file hệ thống.

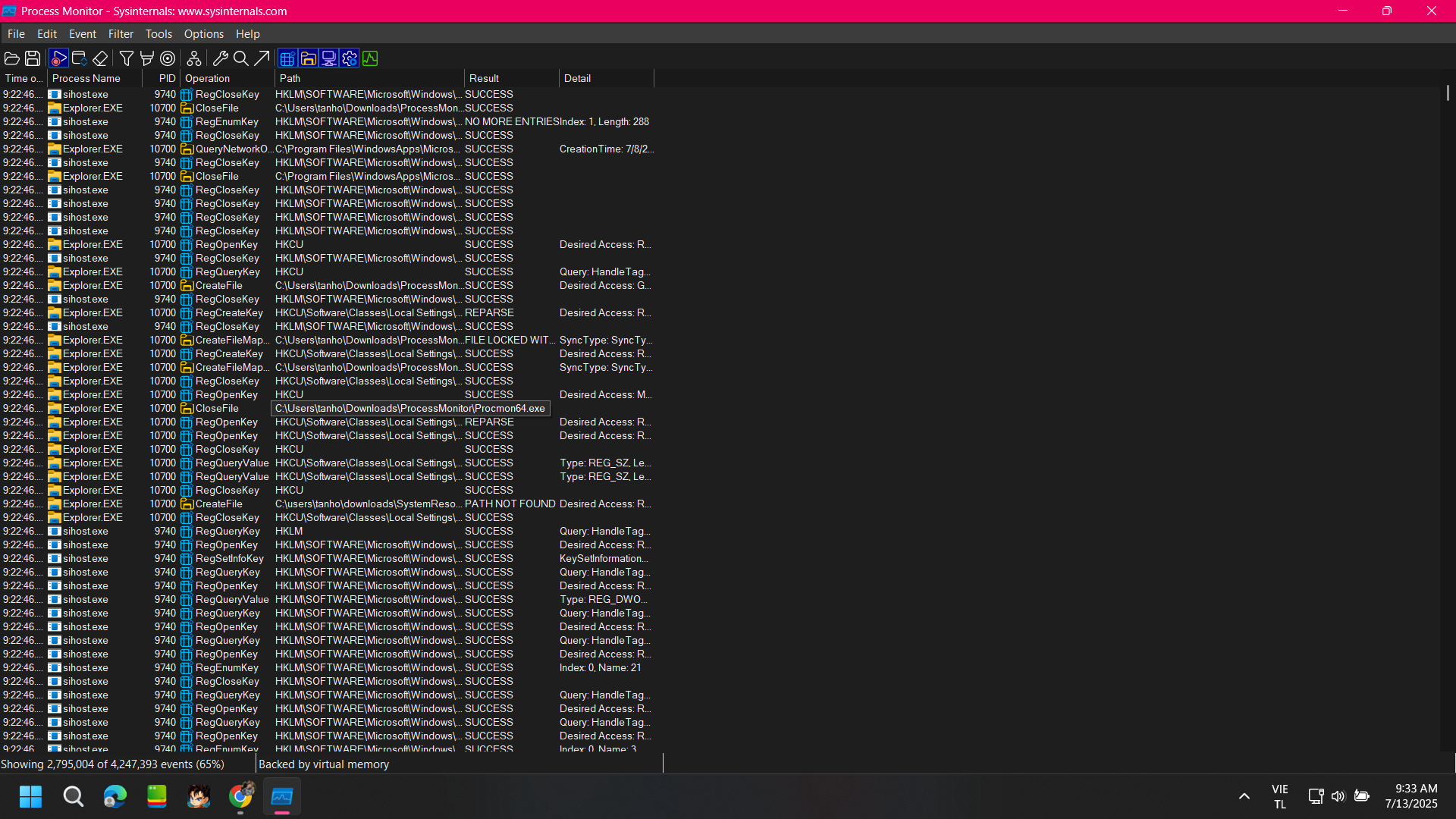
**3. Kết quả thực hành**



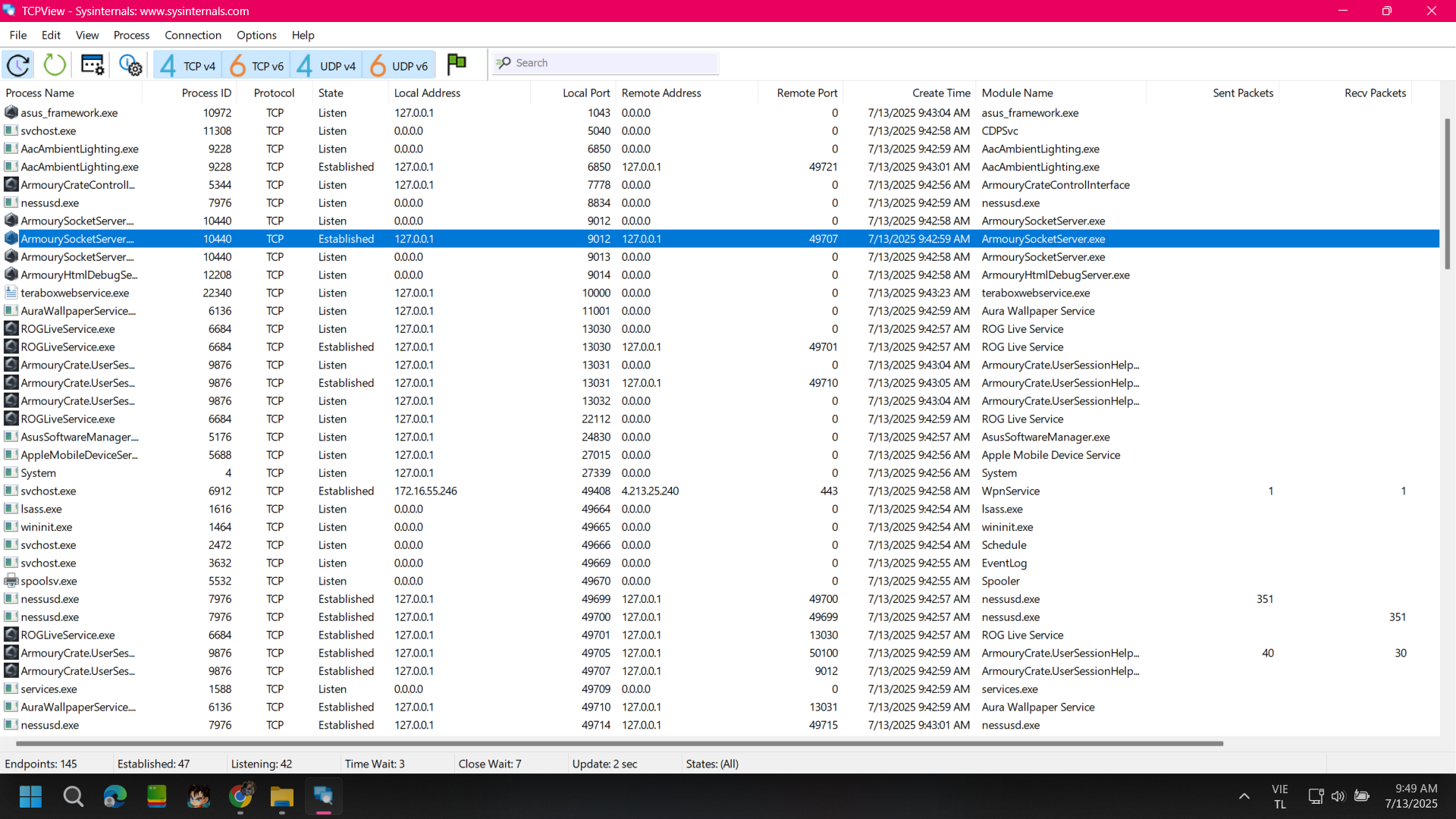
Ảnh 1: Process Explorer – Danh sách tiến trình đang chạy



Ảnh 2: Autoruns – Các chương trình khởi động cùng hệ thống



Ảnh 3: Process Monitor – Theo dõi hoạt động tiến trình



Ảnh 4: TCPView – Kiểm tra kết nối mạng từ tiến trình

**4. Đánh giá và kết luận**  
Qua quá trình sử dụng các công cụ Sysinternals, đã phát hiện một số tiến trình và hành vi bất thường như:  
- Một số tiến trình không có chữ ký số rõ ràng hoặc không tìm thấy mô tả đầy đủ.  
- Một số mục trong Autoruns dẫn tới file không tồn tại hoặc chạy từ thư mục tạm thời.  
- Process Monitor hiển thị các thao tác can thiệp registry và hệ thống file.  
- TCPView ghi nhận các tiến trình kết nối tới địa chỉ mạng nội bộ, một số tiến trình mở cổng lạ.