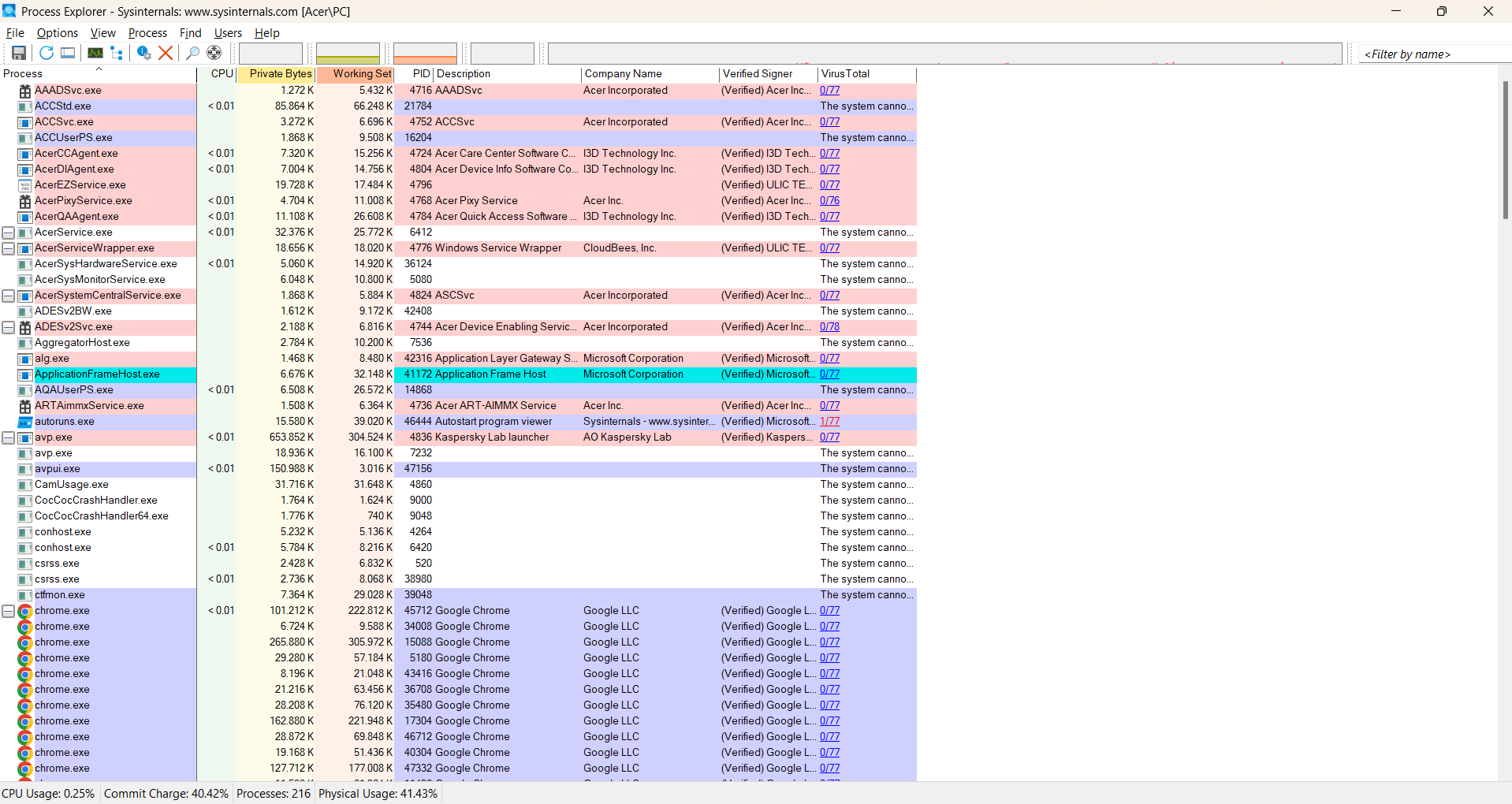
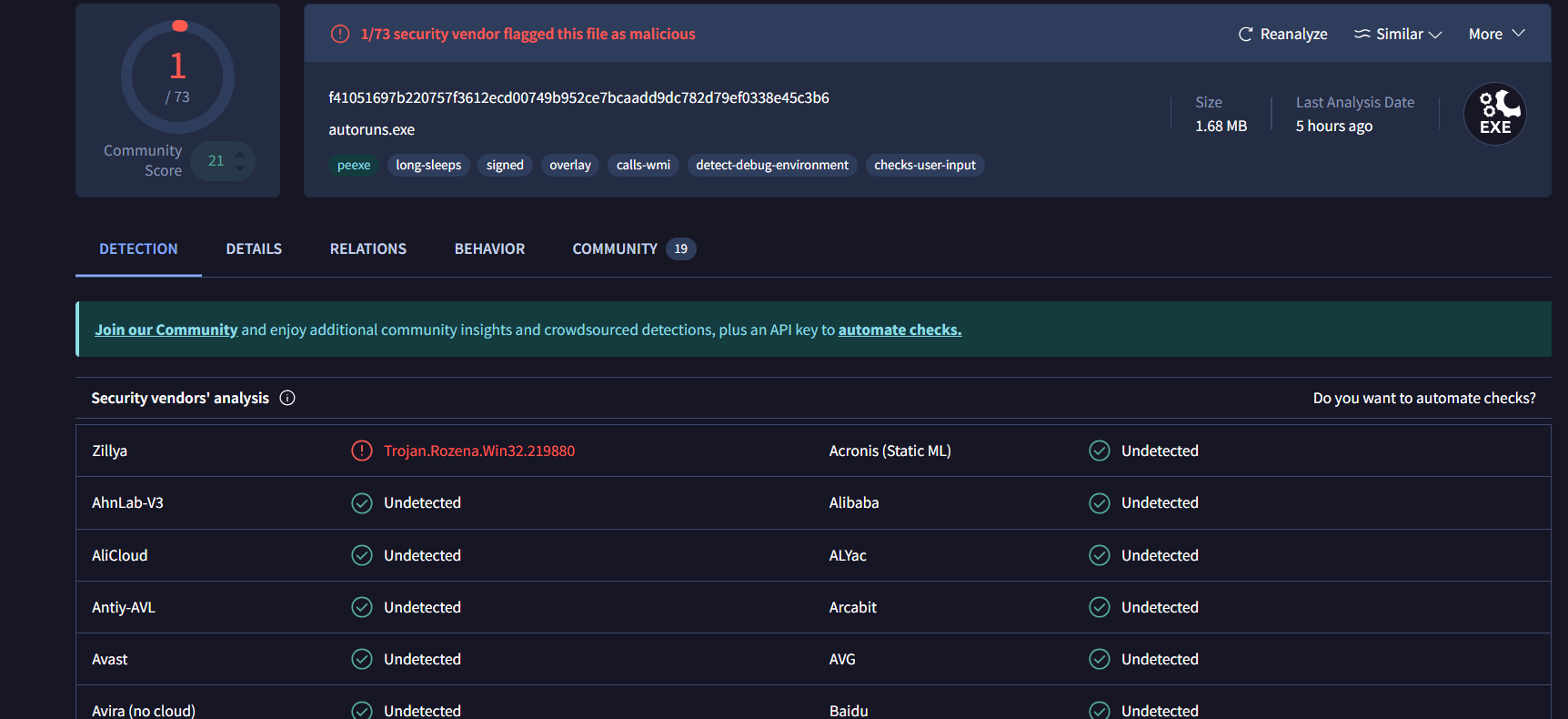
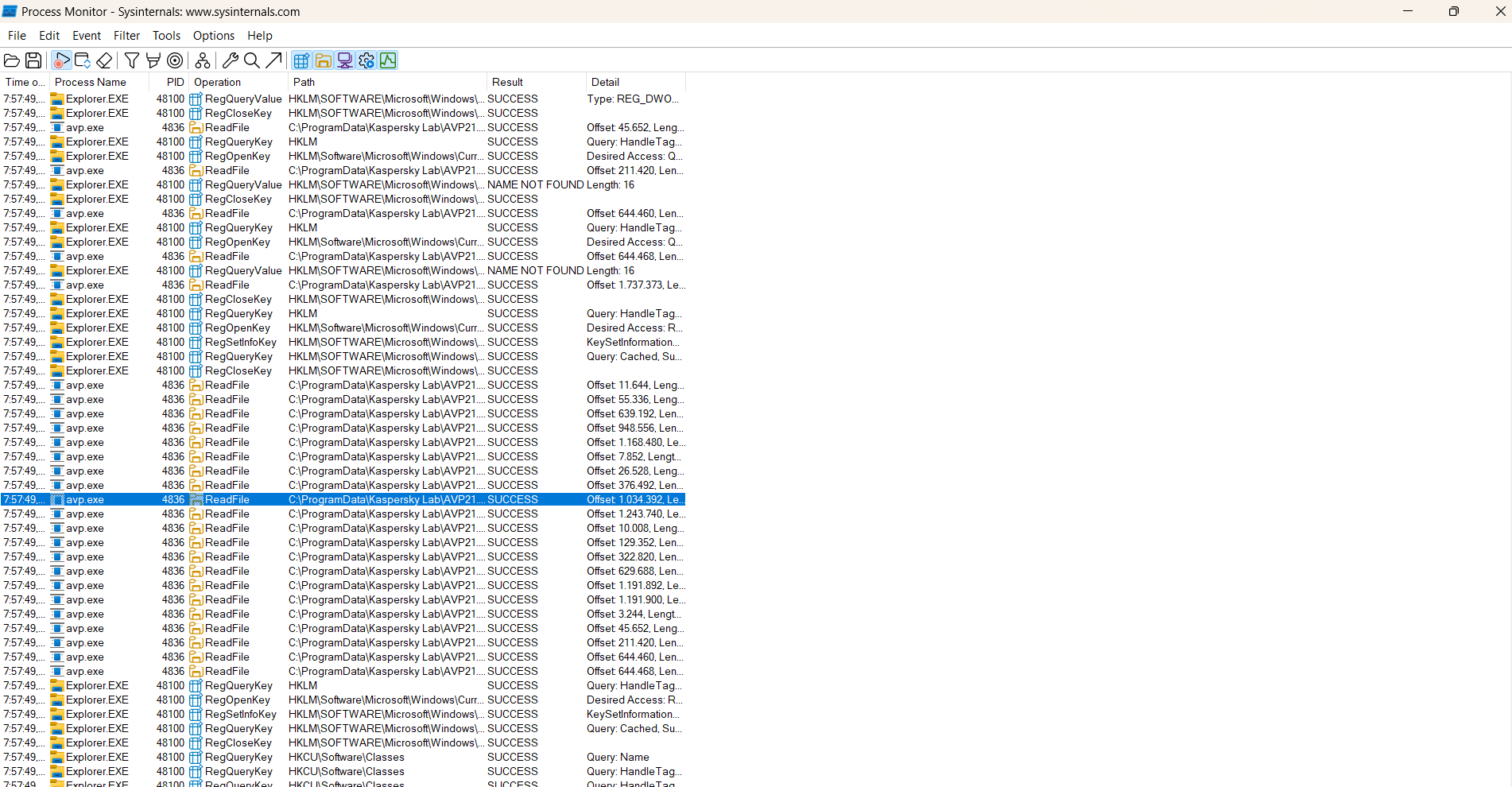
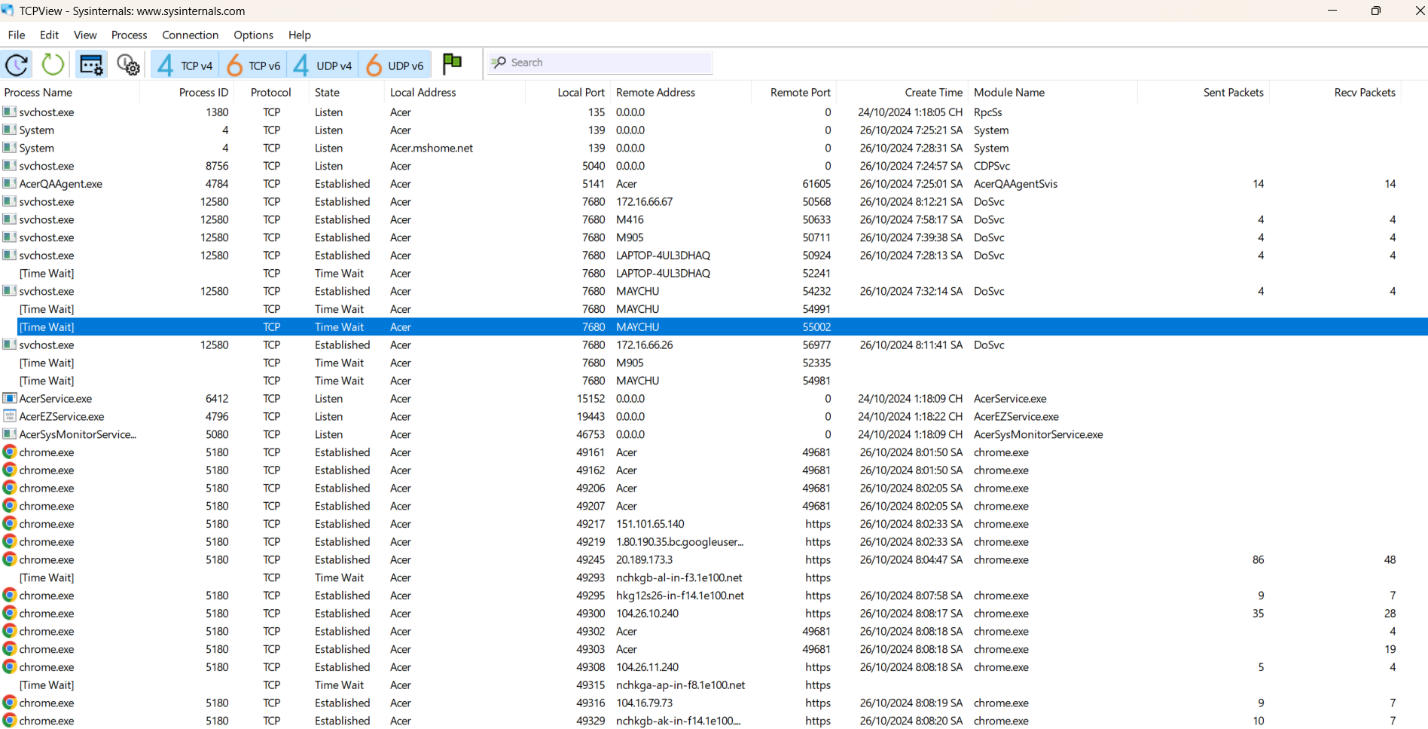
**1. Hiển thị thông tin các tiến trình: Process Explorer**

1. **Xác định các chương trình chạy tự động: Autorun**



1. **Theo dõi hoạt động của Malware :Process Monitor**

1.  **Xác định xem tiến trình nào đang sinh ra hoạt động mạng tương ứng TCPview**

1. **Kiểm tra dữ liệu mã độc đã gửi và nhận Wireshark**

