**Họ và tên: Tăng Dũng Cẩm**

**MSSV: 22520141**

1. **Nêu các biện pháp phòng chống Trojan, sắp xếp theo thứ tự các biện pháp quan trọng từ cao đến thấp.**

Các biện pháp phòng chống Trojan được sắp xết theo thứ tự quan trọng từ cao đến thấp:

1. **Cài đặt bản vá và cập nhật bảo mật cho hệ điều hành và ứng dụng** (Install patches and security updates for the operating systems and applications).
2. **Chặn tất cả các cổng không cần thiết tại host và tường lửa** (Block all unnecessary ports at the host and firewall).
3. **Hạn chế quyền trong môi trường máy tính để bàn để ngăn chặn cài đặt ứng dụng độc hại** (Restrict permissions within the desktop environment to prevent malicious applications installation).
4. **Sử dụng phần mềm diệt virus để quét các đĩa CD và DVD trước khi sử dụng** (Scan CDs and DVDs with antivirus software before using).
5. **Giám sát lưu lượng mạng nội bộ để phát hiện các cổng hoặc lưu lượng mã hóa bất thường** (Monitor the internal network traffic for odd ports or encrypted traffic).
6. **Chạy phần mềm diệt virus dựa trên host, tường lửa và phần mềm phát hiện xâm nhập** (Run host-based antivirus, firewall, and intrusion detection software).
7. **Quản lý tính toàn vẹn của máy trạm qua các công cụ như checksums, auditing, và port scanning** (Manage local workstation file integrity through checksums, auditing, and port scanning).
8. **Tránh tải xuống và thực thi ứng dụng từ các nguồn không đáng tin cậy** (Avoid downloading and executing applications from untrusted sources).
9. **Hạn chế việc sử dụng các tập lệnh hoặc lệnh có sẵn mà không hiểu rõ** (Avoid typing commands blindly and implementing pre-fabricated programs or scripts).
10. **Không chấp nhận các chương trình chuyển qua tin nhắn tức thời** (Avoid accepting programs transferred by instant messaging).
11. **Tránh mở các tệp đính kèm email từ người gửi không rõ nguồn gốc** (Avoid opening email attachments received from unknown senders).
12. **Tăng cường cấu hình mặc định yếu và vô hiệu hóa chức năng không cần thiết** (Harden weak, default configuration settings and disable unused functionality including protocols and services).
13. **Cho biết công dụng và cách sử dụng một số công cụ sau: Netstat, Fport, TCPView, CurrPorts Tool, Process Explorer (hoặc công cụ khác có chức năng tương tự). So sánh sự khác biệt giữa các công cụ này.**

**Netstat:**

* **Công dụng:**
* Kiểm tra kết nối mạng đang hoạt động: Hiển thị danh sách các kết nối mạng hiện có trên máy, bao gồm các thông tin như địa chỉ IP và cổng.
* Xem các cổng mở trên hệ thống: Kiểm tra các cổng mạng mở trên máy tính để phát hiện các dịch vụ hoặc ứng dụng đang lắng nghe trên các cổng đó.
* Giám sát lưu lượng mạng: Hỗ trợ quản trị viên mạng theo dõi và giám sát lưu lượng mạng để phát hiện các kết nối không mong muốn hoặc nguy hiểm.
* Chẩn đoán sự cố mạng: Giúp phát hiện các vấn đề về kết nối mạng và hỗ trợ chẩn đoán lỗi mạng.
* **Cấu trúc của lệnh:**

NETSTAT [-a] [-b] [-e] [-f] [-i] [-n] [-o] [-p *Protocol* ] [-r] [-s] [-t] [-x] [-y] [*interval*] [/?]

* Trong đó các lựa chọn:

-a: Hiển thị tất cả các kết nối và cổng đang lắng nghe.

-n: Hiển thị các địa chỉ và số cổng ở dạng số (không phân giải DNS), giúp lệnh thực thi nhanh hơn.

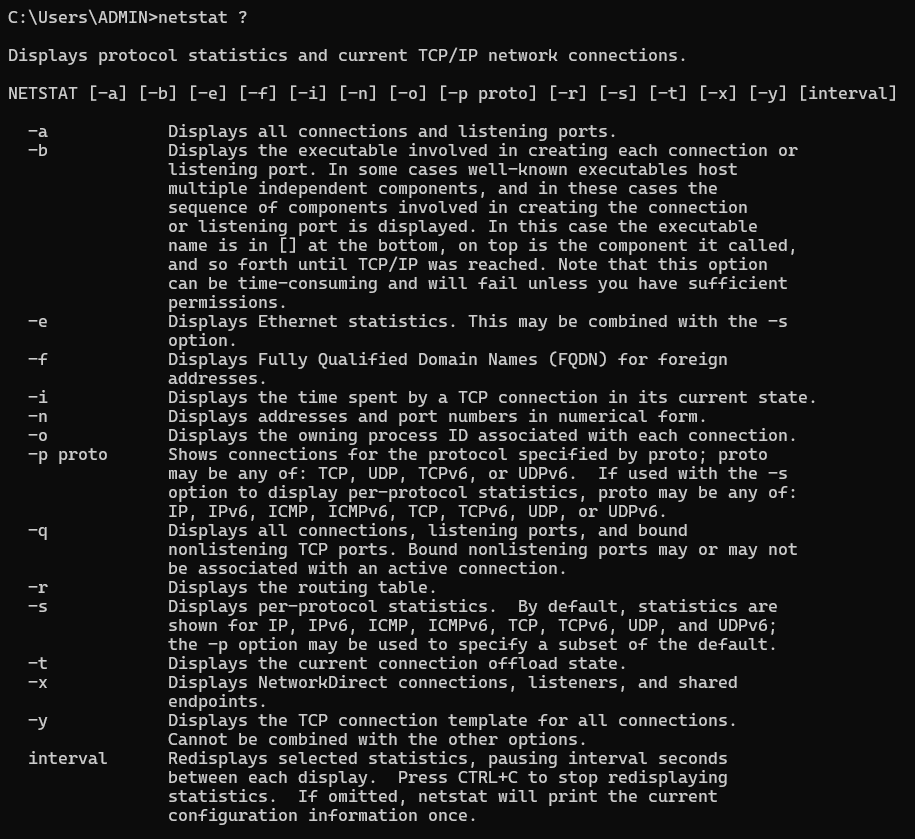
-o (Windows): Hiển thị thêm ID của tiến trình (PID) sử dụng kết nối mạng đó.

-b (Windows, yêu cầu quyền admin): Hiển thị các tên chương trình đang kết nối, hữu ích khi muốn xem chương trình nào đang mở cổng cụ thể.

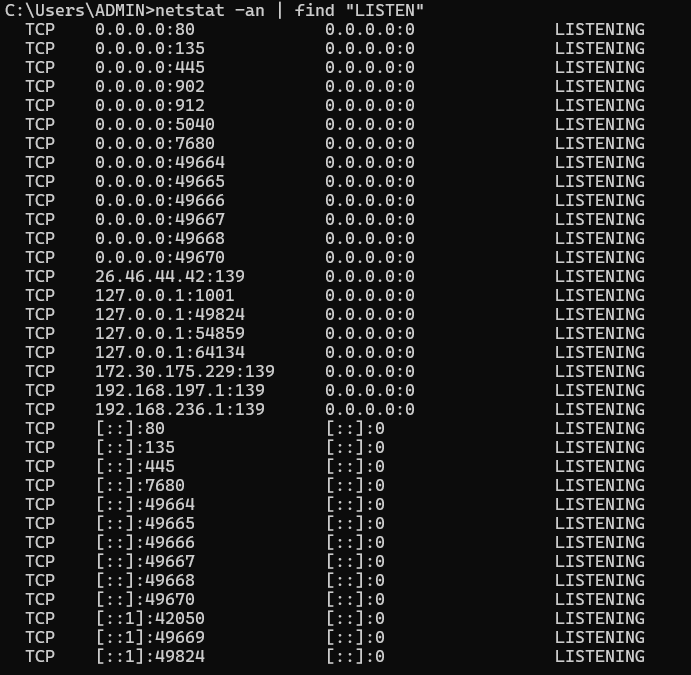
-s: Hiển thị thống kê cho từng giao thức như TCP, UDP, ICMP.

-r: Hiển thị bảng định tuyến (routing table) của hệ thống.

-p <protocol>: Lọc kết quả theo giao thức, ví dụ netstat -p tcp để hiển thị kết nối TCP, hoặc netstat -p udp cho kết nối UDP.

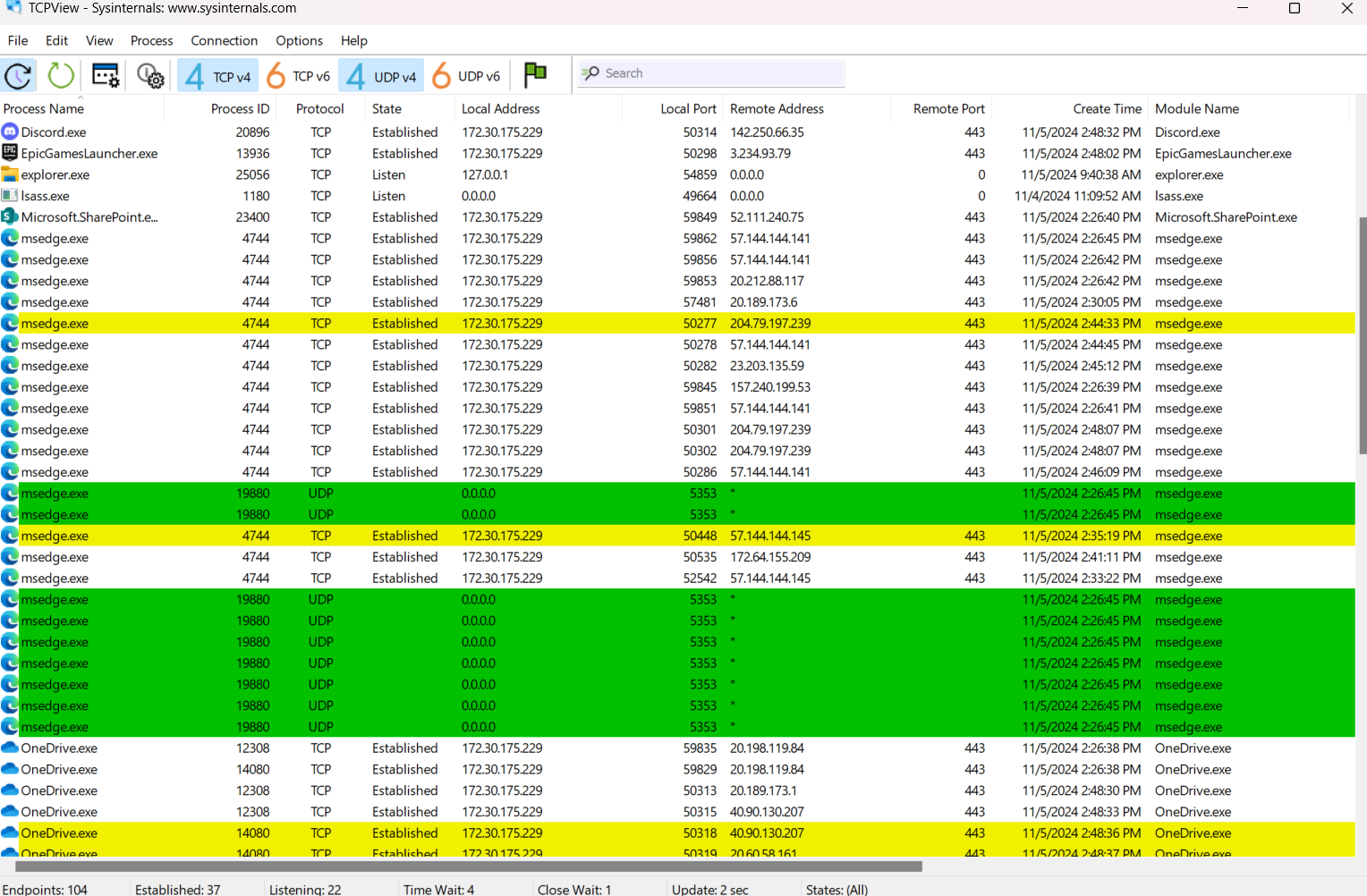


* Ví dụ: liệt kê tất cả các cổng đang lắng nghe (LISTENING) trên máy tính.

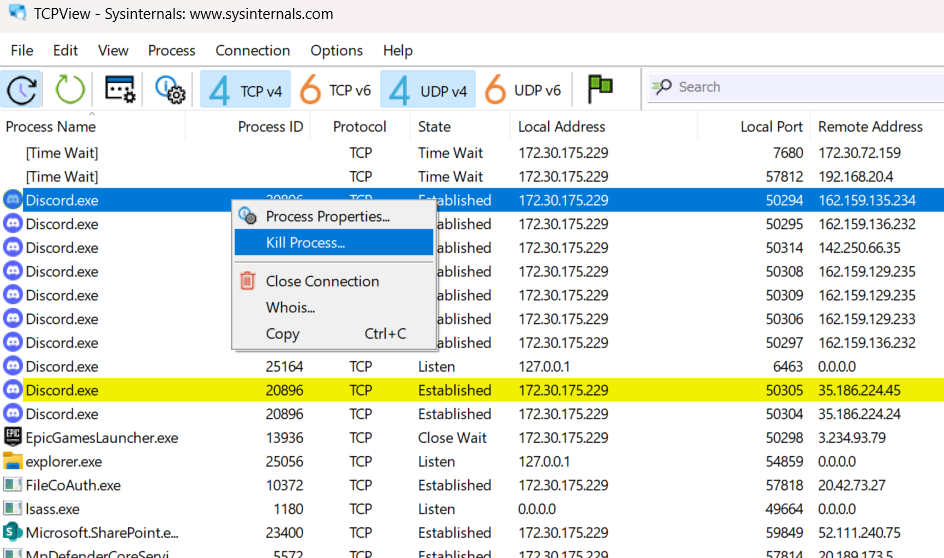


**TCPView:**

* **Công dụng**:
* Giám sát kết nối mạng trực tiếp: TCPView hiển thị thông tin về các kết nối TCP và UDP đang hoạt động, giúp dễ dàng theo dõi tình trạng kết nối mạng.
* Kiểm tra chi tiết kết nối: Cung cấp các chi tiết quan trọng như địa chỉ IP nguồn và đích, số cổng, giao thức, và trạng thái kết nối (Established, Listening, Closed, ...).
* Quản lý và đóng các kết nối không mong muốn: Người dùng có thể xác định và đóng bất kỳ kết nối nào, giúp bảo vệ máy tính khỏi các mối đe dọa an ninh mạng hoặc các phần mềm không mong muốn.
* Theo dõi tiến trình: Hiển thị ứng dụng hoặc tiến trình nào đang sử dụng kết nối mạng đó, giúp xác định các ứng dụng đang kết nối ra bên ngoài.
* Phát hiện các kết nối bất thường: Có ích trong việc phát hiện các hoạt động mạng không mong muốn từ phần mềm độc hại, Trojan, hoặc các tiến trình không xác định.
* **Cách sử dụng:**

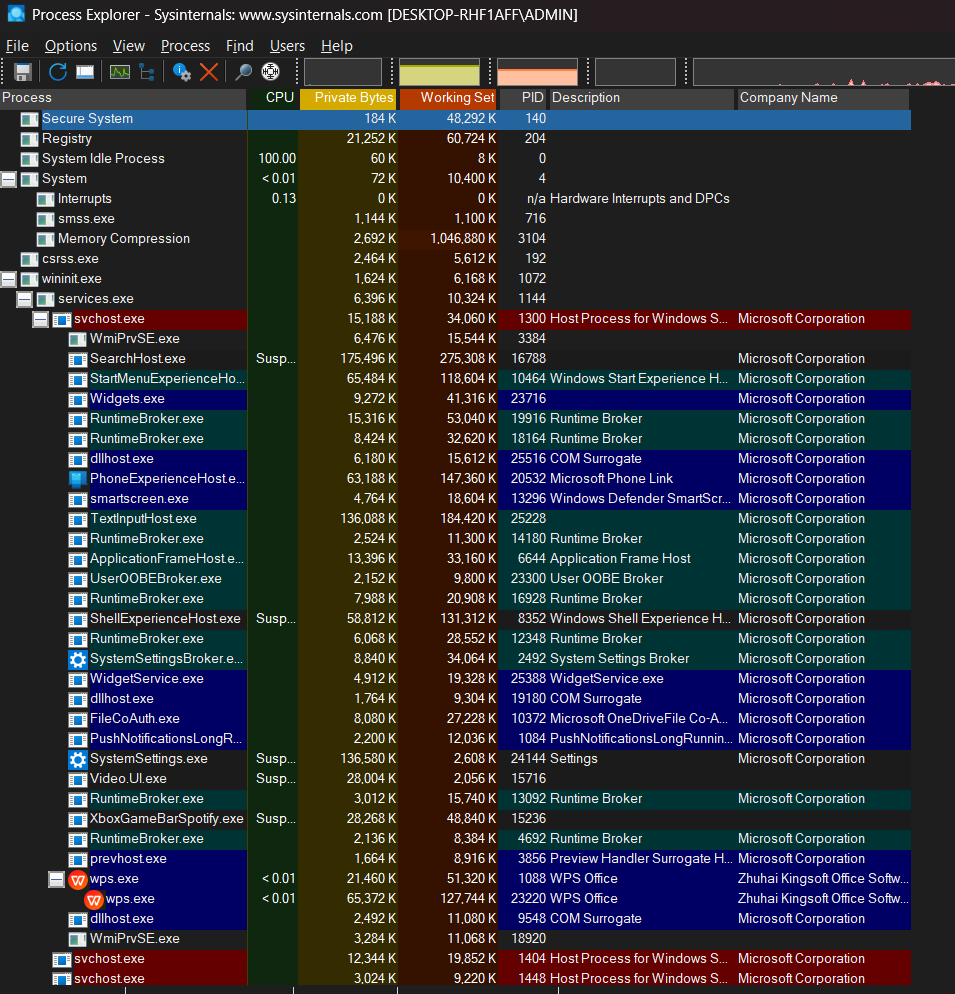


* **Cột Process**: Hiển thị tên tiến trình đang sử dụng kết nối mạng.
* **Cột PID**: ID của tiến trình giúp bạn dễ dàng tìm tiến trình trong Task Manager.
* **Cột Protocol**: Hiển thị giao thức mạng được sử dụng, chẳng hạn như TCP hoặc UDP.
* **Cột Local Address và Local Port:** Địa chỉ IP và cổng trên máy tính của bạn.
* **Cột Remote Address và Remote Port**: Địa chỉ IP và cổng của điểm đích mà máy tính của bạn kết nối đến.
* **Cột State**: Trạng thái của kết nối, ví dụ như Listening, Established, Time Wait, hoặc Closed.
* **Các thao tác trong chương trình:**
* **Đóng kết nối**: Nhấp chuột phải vào bất kỳ kết nối nào và chọn Close Connection để đóng kết nối đó. Đây là cách hữu ích để ngắt kết nối từ các tiến trình không mong muốn.
* **Đóng tiến trình**: Bạn cũng có thể chọn End Process để kết thúc tiến trình hoàn toàn nếu bạn nghi ngờ đó là phần mềm độc hại hoặc ứng dụng không mong muốn.
* **Cấu hình cập nhật**: Vào menu Options để thay đổi tốc độ cập nhật, ví dụ như để cập nhật chậm hơn nếu danh sách kết nối quá dài.

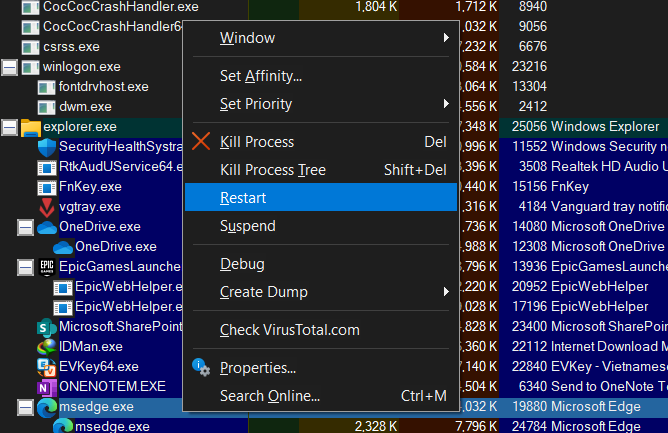


**Process Explorer**

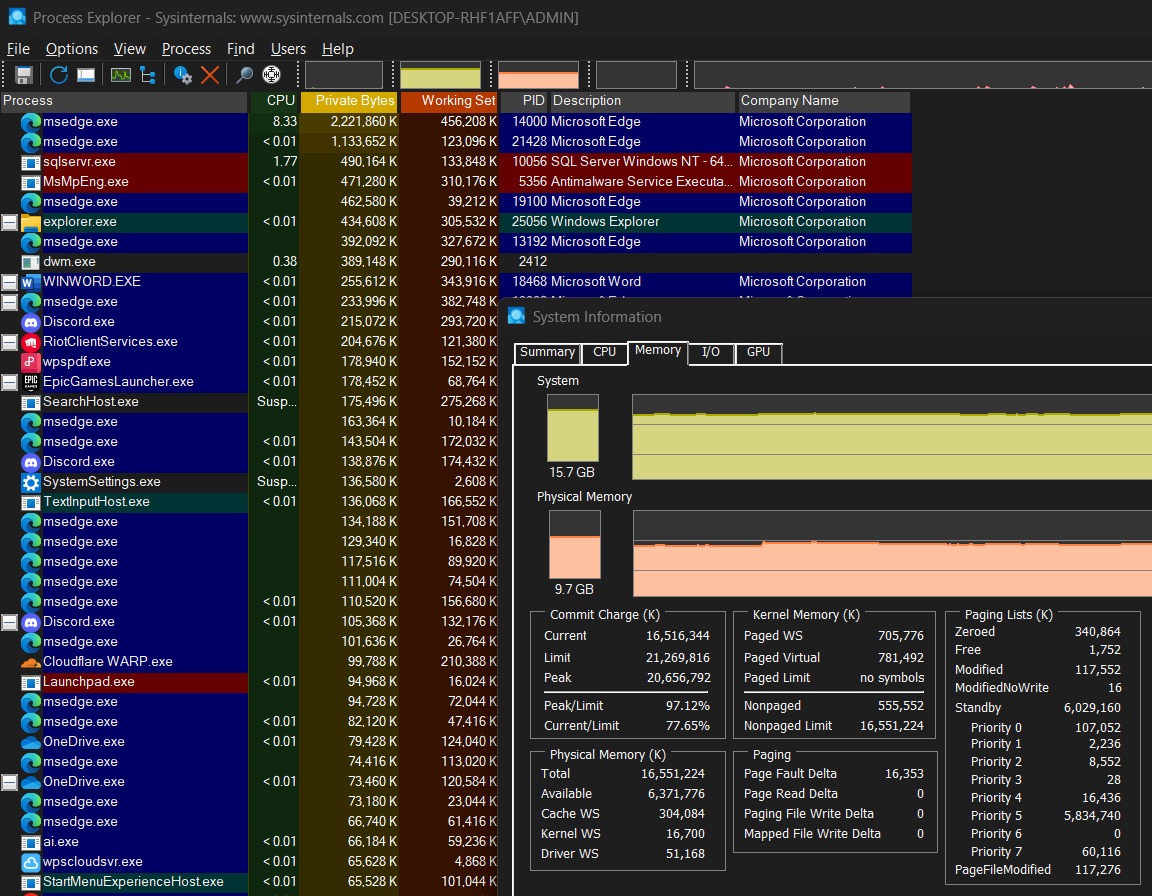
* **Công dụng:**
* **Hiển thị thông tin chi tiết về các tiến trình:** Process Explorer cho phép bạn xem danh sách các tiến trình đang chạy trên hệ thống, bao gồm tên tài khoản sở hữu và các thông tin chi tiết khác.
* **Xem các handle và DLL:** Công cụ này cho phép bạn xem các handle và DLL mà các tiến trình đã mở hoặc tải. Điều này rất hữu ích để theo dõi các vấn đề về phiên bản DLL hoặc rò rỉ handle.
* **Tìm kiếm mạnh mẽ:** Process Explorer có khả năng tìm kiếm mạnh mẽ, giúp bạn nhanh chóng xác định các tiến trình nào đã mở các handle cụ thể hoặc tải các DLL cụ thể.
* **Chẩn đoán và khắc phục sự cố:** Công cụ này giúp bạn theo dõi và khắc phục các vấn đề liên quan đến phiên bản DLL hoặc rò rỉ handle, cung cấp cái nhìn sâu sắc về cách Windows và các ứng dụng hoạt động



* **Cách sử dụng:**
* **Đóng tiến trình:** Nhấp chuột phải vào một tiến trình và chọn Kill Process để dừng tiến trình đó.
* **Tạm dừng tiến trình:** Có thể chọn Suspend để tạm dừng tiến trình mà không kết thúc hẳn, dùng khi cần kiểm tra ảnh hưởng của tiến trình.

****

* **Chế độ handle và DLL**: Bạn có thể chuyển đổi giữa chế độ handle và DLL để xem các handle hoặc DLL mà tiến trình đã mở hoặc tải.
* **Tìm kiếm handle và DLL**: Sử dụng biểu tượng kính lúp trên thanh công cụ để tìm kiếm các handle hoặc DLL cụ thể.
* **Khắc phục sự cố**: Sử dụng Process Explorer để theo dõi và khắc phục các vấn đề liên quan đến phiên bản DLL hoặc rò rỉ handle
* **Sắp xếp theo tài nguyên**: Người dùng có thể sắp xếp tiến trình theo CPU, Memory, hoặc I/O để nhanh chóng xác định tiến trình tiêu tốn tài nguyên.

****

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Công cụ** | **Giao diện** | **Chức năng chính** | **Ưu điểm** | **Nhược điểm** |
| **Netstat** | Dòng lệnh | Hiển thị các kết nối mạng đang hoạt động, các cổng mở, địa chỉ IP, giao thức, trạng thái kết nối | - Có sẵn trên hầu hết các hệ điều hành (Windows, Linux, macOS) | - Giao diện dòng lệnh khó sử dụng cho người mới bắt đầu |
|  |  |  | - Không cần cài đặt thêm phần mềm | - Không cung cấp thông tin chi tiết về tiến trình sử dụng kết nối |
|  |  |  | - Hiệu quả trong việc chẩn đoán các vấn đề mạng cơ bản | - Khó theo dõi và quản lý các kết nối mạng phức tạp |
| **TCPView** | Đồ họa | Theo dõi và quản lý các kết nối mạng TCP và UDP | - Giao diện đồ họa dễ sử dụng | - Chỉ dành cho Windows |
|  |  |  | - Cung cấp thông tin chi tiết và trực quan về các kết nối mạng | - Không cung cấp thông tin chi tiết về tiến trình |
|  |  |  | - Dễ dàng đóng các kết nối không mong muốn | - Không hỗ trợ các hệ điều hành khác ngoài Windows |
| **Process Explorer** | Đồ họa | Quản lý và giám sát các tiến trình đang chạy, xem các handle và DLL mà tiến trình đã mở hoặc tải | - Giao diện đồ họa mạnh mẽ và chi tiết | - Chỉ dành cho Windows |
|  |  |  | - Cung cấp thông tin chi tiết về các tiến trình và tài nguyên hệ thống | - Có thể phức tạp đối với người dùng không chuyên |
|  |  |  | - Giúp phát hiện phần mềm độc hại và các vấn đề liên quan đến hệ thống | - Không cung cấp thông tin chi tiết về kết nối mạng |

1. **Tìm kiếm 3-5 loại Trojan mới xuất hiện trong thời gian gần đây. Lập bảng mô tả các Trojan đó (Tên, nguồn gốc, đặc điểm, công xâm nhập, biện pháp phòng chống, nguồn tham khảo...).**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tên Trojan** | **Nguồn gốc** | |  | | --- | | **Đặc điểm** | | **Cổng xâm nhập** | **Biện pháp phòng chống** | **Nguồn tham khảo** |
| SocGholish | Phát hiện từ 2023 | Trojan này được phân phối qua các trang web độc hại, sử dụng các bản cập nhật giả (như cập nhật trình duyệt) để lừa người dùng tải xuống mã độc. | Không xác định | Không mở hoặc cài đặt các bản cập nhật không rõ nguồn gốc, sử dụng phần mềm chống mã độc. | [Top 10 Malware Q3 2023](https://www.cisecurity.org/insights/blog/top-10-malware-q3-2023) |
| Shlayer | Xuất hiện từ 2018, chủ yếu nhắm vào người dùng macOS, vẫn phổ biến năm 2023 | Trojan downloader lây lan qua các liên kết cập nhật giả mạo, đặc biệt là Flash Player. Cài đặt adware và theo dõi hoạt động duyệt web của người dùng để nhắm mục tiêu quảng cáo. | Sử dụng cổng HTTP/HTTPS tiêu chuẩn (80/443) nhưng có thể thay đổi tùy thuộc vào payload được cài đặt. | Tránh tải phần mềm từ các trang web không đáng tin cậy; sử dụng kho ứng dụng chính thức và chương trình chống virus đáng tin cậy trên macOS. Nâng cao nhận thức về các kỹ thuật lừa đảo xã hội để phòng tránh. | [Shlayer Malware Analysis - Acronis](https://www.acronis.com/en-us/blog/posts/shlayer-malware/) |
| AndroxGh0st | Phát hiện khoảng năm 2022 | Một loại RAT (Remote Access Trojan) tinh vi cho Android, có thể kiểm soát chức năng thiết bị, thu thập dữ liệu, chụp ảnh màn hình và ghi âm. Phổ biến qua các tệp APK độc hại từ các liên kết lừa đảo và cửa hàng ứng dụng không chính thức. | Không có cổng cụ thể vì khai thác qua quyền truy cập thiết bị; hoạt động qua các kết nối mạng di động. | Tránh tải APK từ các nguồn không đáng tin cậy; kích hoạt tính năng Play Protect trên Android;​  [Red Canary](https://redcanary.com/threat-detection-report/threats/shlayer/)  phòng chống virus cho thiết bị di động. | [Shlayer - Red Canary Threat Detection Report](https://redcanary.com/threat-detection-report/threats/shlayer/) |
| AsyncRAT | Được phát triển và lây lan mạnh mẽ, đặc biệt là trong năm 2023 | Một RAT đa chức năng cho phép keylogging, điều khiển từ xa và quản lý tệp. Phân phối qua các tệp đính kèm email và liên kết lừa đảo, chủ yếu nhắm vào hệ thống Windows. | Thường sử dụng các cổng phổ biến như 80, 443 cho giao tiếp HTTP/HTTPS, tùy vào cấu hình của kẻ tấn công. | Tránh mở các tệp đính kèm và liên kết email đáng ngờ, sử dụng bộ lọc email​  , sử dụng hệ thống phát hiện xâm nhập để giám sát lưu lượng mạng bất thường. | [Shlayer Trojan – How a Social Engineering Attack Is Targeting 10% of Macs](https://www.macupdate.com/how-to/shlayer-trojan-mac), [Shlayer - Red Canary Threat Detection Report](https://redcanary.com/threat-detection-report/threats/shlayer/) |

**THAM KHẢO**

**[1]** [**easeus.com**](https://www.easeus.com/knowledge-center/netstat-command.html#:~:text=Step%201%3A%20Open%20the%20start,%2C%20just%20type%20netstat%20%2Da.)

**[2]** [**TCPView for Windows - Sysinternals | Microsoft Learn**](https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview)

**[3]** [**Process Explorer - Sysinternals | Microsoft Learn**](https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer)