# Bài tập ngày 21/4/2025

1. Liệt kê các biện pháp phòng chống Trojan và Virus theo thứ tự ưu tiên từ cao đến thấp.

Một số biện pháp phòng chống Trojan:

- Scan for suspicious OPEN PORTS
- Scan for suspicious RUNNING PROCESSES
- Scan for suspicious REGISTRY ENTRIES
- Scan for suspicious DEVICE DRIVERS
- Scan for suspicious WINDOWS SERVICES
- Scan for suspicious STARTUP PROGRAMS
- Scan for suspicious FILES and FOLDERS
- Scan for suspicious NETWORK ACTIVITIES
- Scan for suspicious modification to OPERATING SYSTEM FILES
- Run Trojan SCANNER to detect Trojans

Một số biện pháp phòng chống Virus

- Cài đặt và sử dụng phần mềm diệt virus
- Sao lưu dữ liệu thường xuyên
- Hạn chế sử dụng thiết bị lưu trữ không rõ nguồn gốc.
- Không mở email hoặc tệp đính kèm từ nguồn không tin cậy.
- Không cài đặt phần mềm không có bản quyền hoặc tải từ nguồn không đáng tin.
- Cập nhật hệ điều hành và phần mềm thường xuyên.
- Sử dụng tường lửa và công cụ bảo mật mạng.
- Quét hệ thống định kỳ
- Giám sát hoạt động mạng
- Nâng cao nhận thức bảo mật

2. Tìm và nêu đặc điểm của 6 loại mã độc (2 virus, 2 worm, 2 trojan) xuất hiện trong thời gian gần đây (ghi chú nguồn tham khảo).

| Mã độc | Loại mã độc | Đặc điểm | Nguồn |
|---|---|---|---|

| | | | |
|---|---|---|---|
| LockBit 3.0 | Virus | Là ransomware hoạt động từ năm 2020, thiết kế modular, khó phát hiện. Sử dụng kỹ thuật "double extortion" (mã hóa dữ liệu và đánh cắp dữ liệu nhạy cảm để đe dọa rò rỉ). Đã tấn công các tổ chức lớn như Maximum Industries và TSMC, yêu cầu tiền chuộc lớn. | https://www.avast.com/c-new-computer-viruses |
| Clop | Virus | Là phiên bản hiện đại của CryptoMix, nhắm vào Windows, mã hóa tệp và chặn hơn 600 quy trình hệ thống. Đã tấn công các tổ chức như Đại học Maastricht và Johns Hopkins, khai thác lỗ hổng MOVEit qua SQL injection. | https://www.avast.com/c-new-computer-viruses |
| CMoon | Worm | Worm dựa trên .NET, phát hiện tháng 7/2024, chủ yếu tại Nga, lan truyền qua trang web bị xâm nhập. Có khả năng đánh cắp dữ liệu bảo mật, tải thêm mã độc, phát động DDoS, giám sát USB và chụp ảnh màn hình. | https://cybersecuritynews.com/new-cmoon-worm-attacking |
| SSH-Snake | Worm | Worm tự sửa đổi, phát hiện năm 2024, đánh cắp khóa SSH để lan truyền qua mạng, ánh xạ mạng cho di chuyển ngang, tránh phát hiện bằng cách loại bỏ mẫu tấn công kịch bản hóa. | https://www.bleepingcomputer.com/news/security/new-ssh-snake-malware-steals-ssh-keys-to-spread-across-the-network/ |
| SocGholish | Trojan | Downloader/Trojan, chiếm 60% trong top 10 mã độc đầu năm 2024, hoạt động từ 2017, phân phối qua drive-by-download, triển khai RATs. | https://www.avast.com/c-new-computer-viruses |
| Zeus Gameover | Trojan | Thuộc gia đình Zeus, đánh cắp thông tin tài khoản ngân hàng, hoạt động như botnet peer-to-peer, khó theo dõi, do Evgeniy Bogachev tạo ra. | https://www.safetydetectives.com/blog/most-dangerous-new-malware-and-security-threats/ |