Vắng: Huỳnh Ngọc Bảo Châu (21520643)

Câu 1. Mô tả tính chất cơ bản của virus máy tính.

* Lây lan: virus máy tính lây nhiễm nhiều cách thức khác nhau, virus máy tính có thể sao chép hoặc đính kèm chính nó vào các tệp, chương trình khác để lây lan, đồng thời có thể lây lang từ máy tính này qua máy tính khác
* Phá hoại: virus máy tính có thể làm tổn hại, làm hỏng phần mềm hoặc phá huỷ dữ liệu máy tính, và đánh cắp thông tin.
* Nhỏ gọn: thiết kế nhỏ gọn, khó phát hiện.
* Tương thích: virus máy tính tương thích với một nhóm các đối tượng, khi phù hợp với windows phiên bản này thì có thể tấn công cả những windows phiên bản khác.
* Phát triển kế thừa: virus máy tính được phát triển thêm những phiên bản mới dựa theo những đặc điểm đã có.

Câu 2. Liệt kê các biện pháp phòng chống virus theo thứ tự ưu tiên từ cao đến thấp.

Các biện pháp phòng chống virus theo thứ tự ưu tiên là:

* Cài đặt phần mềm chống virus
* Không mở các tập tin đính kèm từ người gửi không xáy định
* Tuân thủ các chính sách an toàn máy tính
* Chú ý đến ổ đĩa khi tải các tệp tin từ internet về máy
* Cập nhật phần mềm chống virus thường xuyên
* Thường xuyên sao lưu dữ liệu
* Thực hiện quét driver sau mỗi lần cài đặt phần mềm chống virus
* Không chấp nhận ổ đĩa hay chương trình nào mà không kiểm tra chúng khi sử dụng lần đầu tiên

Câu 3. Tìm hiểu và nêu đặc điểm của 4-5 loại mã độc (virus, worm…) xuất hiện trong thời gian gần đây (tên, nguồn gốc, đặt điểm, phương thức phá hoại, biện pháp phòng chống, nguồn tham khảo)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Tên | Nguồn gốc | Đặc điểm | Phương thức phá hoại | Biện pháp phòng chống | Nguồn tham khảo |
| Mouseisland | Hoạt động từ 2019, | Được tìm trong macro của Microsoft | Lừa đảo | Tắt macro cho các ứng dụng microsoft mặc định | [Are MOUSEISLAND malware procedures mitigated on this host? | Chains | Prelude Attack Chains](https://chains.prelude.org/chains/475db1d9-c279-4c7e-a748-8682e1d74ed5/are-mouseisland-malware-procedures-mitigated-on-this-host)  [What Is MOUSEISLAND? (blackberry.com)](https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/mouseisland) |
| Remcos | Breaking Security, Đức | Truy cập từ xa (RAT), được sử dụng để kiểm soát và giám sát hoàn toàn mọi máy tính Windows từ XP trở đi. | Lừa đảo bằng cách thu thập các thông tin sau: thông tin máy tính (hệ điều hành, loại hệ thống, tên sản phẩm), thông tin người dùng, thông tin bổ xử lý rồi gửi về máy chủ của nó thông qua một file đính kèm trên mail | Email scanning  Giải pháp CDR, giải pháp phân tích tên miền để tạo nhiều tên miền nhằm tránh việc chặn các trang web độc hại dựa trên tên miền | [Remcos Malware Information (trendmicro.com)](https://success.trendmicro.com/dcx/s/solution/1123281-remcos-malware-information?language=en_US&sfdcIFrameOrigin=null)  [(1) New Messages! (checkpoint.com)](https://www.checkpoint.com/pt/cyber-hub/threat-prevention/what-is-malware/remcos-malware/#:~:text=Some%20ways%20to%20prevent%20a,malware%20from%20reaching%20users'%20inboxes.) |
| GootLoader | Xuất hiện vào 2020, do nhóm tội phạm Evil Corp phát triển | Dùng để phát tán các loại mã độc khác, như ransomware, trojan, hoặc spyware. | Chiếm quyền điều khiển trang web, tạo các trang web giả mạo | Giải pháp phát hiện và phản hổi điểm cuối EDR, kiểm tra các hệ thống window đã cài đặt, đảm bảo chỉ phần quyền ủy quyền mới được cài đặt | [What Is Gootloader? (blackberry.com)](https://www.blackberry.com/us/en/solutions/endpoint-security/ransomware-protection/gootloader) |
| Emotet (Trojan) | Ukraine, xuất hiện năm 2014 | Đánh cắp thông tin của máy chủ bị nhiễm | Lây nhiễm thông qua macro virus, TrickBot, Qbot trong tệp đính kèm email và các tài liệu độc hại. | Cập nhật định kỳ, không tải tệp tin hoặc truy cập liên kết đáng ngờ. | [Emotet – Wikipedia tiếng Việt](https://en.wikipedia.org/wiki/Emotet) |
| Clop | Nga | Là loại virus mã hoá tệp nguy hiểm . | Có thể lây nhiễm qua nhiều cách khác nhau: email spam, trojan, lỗ hổng…  Sau khi xâm nhập vào hệ thống, ghi đè và thay đổi các tệp hệ thống | Kiểm tra trước khi mở các tệp đính kèm và liên kết.  Tải ứng dụng từ nguồn chính thức.  Cập nhật phần mềm.  Sử dụng phần mềm chống virus. | [What is Clop Ransomware, How It Works and How to Prevent It (heimdalsecurity.com)](https://heimdalsecurity.com/blog/clop-ransomware-overview-operating-mode-prevention-and-removal/#:~:text=Clop%20Ransomware%20belonging%20to%20a,%2C%20databases%20papers%2C%20and%20attach%20.) |