1. Phân tích hiện tượng và loại phần mềm độc hại tương ứng:

|  |  |  |
| --- | --- | --- |
| Hiện tượng | Loại phần mềm độc hại | Giải thích |
| Máy chạy chậm bất thường, quạt kêu to | **Virus hoặc Trojan** | Virus hoặc Trojan chạy ngầm trong hệ thống, chiếm nhiều tài nguyên CPU và bộ nhớ, gây quá tải và làm máy nóng, ồn. |
| Xuất hiện nhiều cửa sổ quảng cáo lạ | **Adware (phần mềm quảng cáo)** | Adware tự động hiển thị quảng cáo, pop-up, hoặc chuyển hướng trình duyệt nhằm thu lợi từ lượt nhấp. |
| Các file bị đổi tên sang đuôi .locked | **Ransomware (mã độc tống tiền)** | Ransomware mã hóa dữ liệu cá nhân và yêu cầu người dùng trả tiền chuộc để mở khóa. |
| Trình duyệt tự mở tab lạ khi khởi động | **Spyware hoặc Adware** | Phần mềm gián điệp hoặc quảng cáo chiếm quyền điều khiển trình duyệt, tự mở các trang web độc hại để theo dõi hành vi người dùng hoặc phát tán mã độc thêm. |

2. Cách xử lý ngay khi phát hiện các dấu hiệu trên:

1. Ngắt kết nối mạng (Internet hoặc Wi-Fi): Giúp ngăn mã độc lan rộng hoặc gửi dữ liệu cá nhân ra ngoài.
2. Khởi động máy tính ở chế độ an toàn (Safe Mode): Tạm thời vô hiệu hóa các tiến trình không cần thiết để dễ dàng quét và loại bỏ phần mềm độc hại.
3. Sử dụng phần mềm diệt virus đáng tin cậy: Quét toàn bộ hệ thống bằng công cụ bảo mật như Windows Defender, Kaspersky, Bitdefender, hoặc Malwarebytes.
4. Không mở hoặc trả tiền chuộc cho ransomware: Giữ nguyên các file bị mã hóa, dùng phần mềm phục hồi dữ liệu hoặc tìm bản sao lưu nếu có.
5. Cập nhật hệ điều hành và phần mềm bảo mật: Vá các lỗ hổng bảo mật để tránh bị tấn công lần sau.
6. Sao lưu dữ liệu định kỳ: Lưu bản sao dữ liệu trên ổ cứng rời hoặc dịch vụ đám mây an toàn để giảm thiểu thiệt hại nếu bị mã độc tấn công.