**Phân Tích Dấu Hiệu và Xử Lý Phần Mềm Độc Hại**

Các hiện tượng máy tính đang gặp phải:

1. Máy chạy chậm bất thường, quạt kêu to.
2. Xuất hiện nhiều cửa sổ quảng cáo lạ.
3. Các file trong máy bị đổi tên sang đuôi **.locked**.
4. Trình duyệt tự động mở tab lạ khi khởi động.

**1. Các loại phần mềm độc hại tương ứng**

Dựa trên các dấu hiệu trên, máy tính của bạn có thể đã bị lây nhiễm ít nhất 3 loại phần mềm độc hại sau:

| STT | Loại phần mềm độc hại | Dấu hiệu tương ứng |
| --- | --- | --- |
| **1** | **Ransomware (Mã độc tống tiền)** | **Các file bị đổi tên sang đuôi .locked.** Đây là dấu hiệu rõ ràng nhất của ransomware, phần mềm đã mã hóa dữ liệu của bạn và yêu cầu tiền chuộc để giải mã. |
| **2** | **Adware (Phần mềm quảng cáo)** | **Xuất hiện nhiều cửa sổ quảng cáo lạ** và **trình duyệt tự động mở tab lạ khi khởi động.** Adware được thiết kế để hiển thị quảng cáo không mong muốn và chuyển hướng trình duyệt. |
| **3** | **Trojan/Rootkit (Phần mềm gián điệp)** | **Máy chạy chậm bất thường, quạt kêu to.** Đây có thể là dấu hiệu của Trojan hoặc Rootkit đang chạy ngầm, chiếm dụng tài nguyên CPU, RAM để thực hiện các hoạt động gián điệp, đào tiền ảo (cryptojacking) hoặc tấn công từ xa. |

**2. Đề xuất cách xử lý ngay lập tức**

Khi phát hiện các dấu hiệu nghiêm trọng như trên, bạn cần thực hiện các bước xử lý khẩn cấp theo thứ tự sau:

1. **Ngắt kết nối mạng ngay lập tức:**
   * **Mục đích:** Ngăn chặn phần mềm độc hại (đặc biệt là Ransomware) tiếp tục lan truyền, mã hóa dữ liệu khác, hoặc gửi thông tin của bạn ra bên ngoài cho tin tặc. Rút dây mạng hoặc tắt Wi-Fi.
2. **Khởi động lại máy ở Chế độ An toàn (Safe Mode):**
   * **Mục đích:** Chỉ tải các chương trình và dịch vụ cơ bản nhất. Điều này giúp ngăn chặn phần mềm độc hại tự khởi động và hoạt động, tạo điều kiện thuận lợi cho việc quét và gỡ bỏ.
3. **Quét và diệt phần mềm độc hại:**
   * Sử dụng phần mềm diệt virus uy tín (như Kaspersky, Bitdefender, Malwarebytes) đã được cập nhật. Thực hiện **quét toàn bộ hệ thống (Full Scan)** để tìm và loại bỏ tất cả các mối đe dọa được phát hiện.
4. **Kiểm tra và khôi phục trình duyệt:**
   * Gỡ bỏ mọi tiện ích mở rộng lạ, đặt lại (reset) cài đặt trình duyệt về trạng thái mặc định để loại bỏ Adware và các thay đổi độc hại.