# Các triệu chứng mô tả có thể do nhiều loại phần mềm độc hại khác nhau gây ra — từ adware, browser hijacker, cryptominer đến ransomware. Hành động nhanh (cô lập thiết bị, ghi bằng chứng, quét bằng công cụ uy tín) kết hợp với phục hồi từ bản sao lưu là con đường an toàn nhất. Phân tích hiện tượng máy bị nhiễm mã độc và cách xử lý

- Máy chạy chậm bất thường, quạt kêu to.

- Xuất hiện nhiều cửa sổ quảng cáo lạ.

- Các file trong máy bị đổi tên sang đuôi .locked.

- Trình duyệt tự động mở tab lạ khi khởi động.

## 1) Ít nhất 3 loại phần mềm độc hại tương ứng

Dưới đây là các loại phần mềm độc hại có khả năng tương ứng với các triệu chứng:

* 1. \*\*Ransomware\*\*

1. - Triệu chứng liên quan: Các file bị đổi tên sang đuôi .locked (hoặc .locked, .crypt, .encrypted...).
2. - Hành vi: Mã hóa file người dùng và yêu cầu tiền chuộc để giải mã.

* 2. \*\*Adware / PUP (Potentially Unwanted Program)\*\*

1. - Triệu chứng liên quan: Nhiều cửa sổ quảng cáo lạ, popup, redirect trình duyệt.
2. - Hành vi: Hiển thị quảng cáo xâm nhập, chèn quảng cáo vào trang web, làm giảm trải nghiệm và đôi khi tải thêm mã độc.

* 3. \*\*Cryptominer (trình khai thác tiền mã hóa trái phép) / Trojan khai thác tài nguyên\*\*

1. - Triệu chứng liên quan: Máy chạy chậm bất thường, CPU/GPU sử dụng cao, quạt kêu to liên tục.
2. - Hành vi: Sử dụng tài nguyên máy để khai thác tiền điện tử cho kẻ tấn công, làm mòn phần cứng và giảm hiệu suất.

* 4. \*\*Browser Hijacker / Extension độc hại\*\*

1. - Triệu chứng liên quan: Trình duyệt tự động mở tab lạ khi khởi động, trang chủ/động cơ tìm kiếm bị đổi.
2. - Hành vi: Thay đổi cài đặt trình duyệt, redirect người dùng tới trang quảng cáo hoặc lừa đảo.

## 2) Đề xuất cách xử lý NGAY KHI PHÁT HIỆN

Ưu tiên: Giữ bình tĩnh — làm theo các bước dưới đây theo thứ tự ưu tiên để giảm thiểu rủi ro và mất mát dữ liệu.

* A. Hành động tức thì (ngắt kết nối và cô lập)

1. - Ngắt kết nối mạng ngay lập tức: rút cáp Ethernet, tắt Wi‑Fi hoặc tháo mô‑đem 4G để ngăn mã độc lan sang thiết bị khác và chặn giao tiếp với máy chủ điều khiển.
2. - Nếu máy là một phần của mạng công ty, báo IT ngay lập tức và rời khỏi mạng để họ xử lý.

* B. Ghi nhận bằng chứng (quan trọng với ransomware)

1. - Chụp màn hình thông báo hay yêu cầu tiền chuộc, danh sách file bị đổi tên, và ghi lại tên phần mở rộng (vd: .locked).
2. - Không xóa các file đã bị mã hóa — giữ nguyên để phục hồi hoặc phân tích forensics.

* C. Không trả tiền chuộc vội vàng

1. - Trả tiền không đảm bảo khôi phục file và khuyến khích kẻ tấn công; cân nhắc tham khảo ý kiến chuyên gia hoặc cơ quan chức năng.

* D. Quét và loại bỏ mã độc

1. - Khởi động vào Safe Mode (Windows) hoặc chế độ an toàn tương ứng và chạy quét toàn bộ bằng phần mềm chống mã độc uy tín (Windows Defender, Malwarebytes, ESET, Kaspersky... ).
2. - Dùng công cụ chuyên dụng để loại bỏ adware/browser hijacker (Malwarebytes AdwCleaner, HitmanPro).
3. - Kiểm tra tiến trình (Task Manager) để phát hiện tiến trình dùng CPU cao; nếu xác định là trình khai thác, kết thúc tiến trình, sau đó quét kỹ.

* E. Xử lý trình duyệt bị chiếm quyền

1. - Mở trình duyệt, vào Extensions/Add-ons, vô hiệu hóa hoặc gỡ bỏ các extension lạ.
2. - Reset cài đặt trình duyệt về mặc định, xóa cache, cookie và lịch sử.

* F. Phục hồi dữ liệu và khôi phục hệ thống

1. - Nếu có backup an toàn (offline hoặc cloud đáng tin cậy), thực hiện khôi phục sau khi máy sạch hoàn toàn.
2. - Nếu không có backup, cân nhắc sử dụng bản sao lưu bản ghi (shadow copies) hoặc tìm chuyên gia phục hồi dữ liệu; với ransomware, khả năng khôi phục không đảm bảo.

* G. Khi biện pháp phần mềm không hiệu quả

1. - Cân nhắc cài đặt lại hệ điều hành (clean install) — đây là cách triệt để nhất để loại bỏ mã độc còn ẩn.
2. - Trước khi cài lại, sao lưu các file quan trọng (không sao lưu các file nghi nhiễm), và chuẩn bị bộ cài sạch từ nguồn chính thức.

* H. Sau khi xử lý — làm sạch và củng cố bảo mật

1. - Cập nhật hệ điều hành và phần mềm lên phiên bản mới nhất; vá lỗ hổng bảo mật.
2. - Thay đổi mọi mật khẩu quan trọng (email, ngân hàng) từ thiết bị an toàn; bật xác thực hai yếu tố (2FA).
3. - Kiểm tra các thiết bị khác trong mạng (điện thoại, máy khác) vì mã độc có thể lan.
4. - Triển khai phần mềm bảo vệ và lên lịch quét định kỳ.

## 3) Lời khuyên phòng ngừa (ngắn gọn)

- Luôn sao lưu định kỳ và giữ bản sao ngoại tuyến (external HDD) hoặc sử dụng backup cloud có phiên bản hóa (versioning).

- Không mở email và tệp đính kèm từ nguồn không rõ; kiểm tra link trước khi click.

- Sử dụng tài khoản người dùng không có quyền admin cho các hoạt động hàng ngày.

- Giữ phần mềm bảo mật và hệ điều hành luôn cập nhật.

## 4) Kết luận