# Phân tích và xử lý khi máy tính có dấu hiệu bị nhiễm phần mềm độc hại

Mô tả tình huống:

"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 có thể tương ứng với các hiện tượng trên

* • Ransomware

- Mô tả: Mã hóa file người dùng và đổi đuôi (ví dụ: .locked), yêu cầu tiền chuộc để giải mã.

- Tương ứng với dấu hiệu: các file bị đổi đuôi .locked.

* • Adware/PUP (Potentially Unwanted Program)

- Mô tả: Hiển thị quảng cáo pop-up, mở tab hoặc cửa sổ quảng cáo liên tục; thường cài kèm phần mềm miễn phí.

- Tương ứng với dấu hiệu: xuất hiện nhiều cửa sổ quảng cáo lạ, trình duyệt tự mở tab lạ.

* • Cryptominer / Trojan (mở cửa hậu)

- Mô tả: Cryptominer sử dụng CPU/GPU để điều khai thác tiền ảo khiến máy chạy chậm và quạt kêu to; Trojan có thể mở cửa hậu để tải về mã độc khác.

- Tương ứng với dấu hiệu: máy chạy chậm bất thường, quạt kêu to do tải CPU/GPU cao.

* • Spyware / Keylogger

- Mô tả: Thu thập thông tin người dùng (mật khẩu, lịch sử), hoạt động ẩn; đôi khi đi kèm với trojan.

- Tương ứng với dấu hiệu: có thể kèm theo hành vi bất thường của trình duyệt hoặc kết nối ra ngoài.

## 2. Tin tặc có thể lợi dụng như thế nào

• Lợi dụng file bị mã hóa (ransomware): ép nạn nhân trả tiền chuộc để đổi lấy công cụ/khóa giải mã; nếu trả có thể vẫn bị lộ dữ liệu hoặc tiếp tục bị tấn công.

• Lợi dụng adware/spyware: thu thập thói quen lướt web, thông tin đăng nhập, dùng để chiếm đoạt tài khoản hoặc bán dữ liệu.

• Lợi dụng cryptominer/trojan: sử dụng tài nguyên máy để trộm lợi nhuận (khai thác tiền ảo) hoặc làm cửa hậu cho các cuộc tấn công sâu hơn.

• Phát tán sang mạng nội bộ: nhiều loại mã độc có thể lây lan sang các máy khác trên cùng mạng (đặc biệt là ransomware), gây hại tập thể.

## 3. Đề xuất cách xử lý NGAY KHI PHÁT HIỆN

1. Cách ly thiết bị ngay lập tức:

- Ngắt kết nối Internet (rút cáp mạng hoặc tắt Wi‑Fi) và rút mọi ổ cứng/USB ngoài để tránh lây lan.

- Nếu máy là phần của hệ thống công ty, thông báo ngay cho bộ phận IT để họ cách ly mạng.

1. Ngừng tương tác và chụp lại bằng chứng:

- Không bấm vào các popup, không nhập mật khẩu hay trả tiền chuộc ngay lập tức.

- Chụp ảnh màn hình hoặc ghi lại thông báo lỗi/đòi tiền chuộc để phục vụ điều tra và khôi phục.

1. Sử dụng thiết bị sạch để thay đổi mật khẩu quan trọng:

- Dùng một máy khác mà bạn biết là an toàn để đổi mật khẩu email, ngân hàng, mạng xã hội nếu nghi ngờ bị lộ.

1. Quét bằng phần mềm chống malware uy tín:

- Khởi động vào Safe Mode (Windows) hoặc chế độ an toàn, chạy quét toàn bộ bằng Windows Defender và một phần mềm chống malware (ví dụ: Malwarebytes) để phát hiện và loại bỏ mã độc.

- Lưu ý: với ransomware, công cụ chống malware có thể không khôi phục file đã bị mã hóa—chỉ giúp loại bỏ phần mềm độc hại.

1. Kiểm tra các chương trình khởi động và tiện ích mở rộng trình duyệt:

- Vào Task Manager → Startup để tắt các tiến trình lạ; vào trình duyệt → Extensions/Add‑ons để gỡ bỏ các tiện ích lạ.

1. Phục hồi từ bản sao lưu an toàn:

- Nếu có bản sao lưu (backup) gần nhất và đảm bảo backup không bị lây nhiễm, phục hồi hệ thống và file từ backup.

- Nếu là ransomware, KHÔNG trả tiền chuộc vội vàng — hãy tham khảo chuyên gia và cơ quan chức năng; kiểm tra bản giải mã có sẵn từ cộng đồng bảo mật.

1. Cân nhắc cài lại hệ điều hành nếu cần:

- Nếu mã độc khó diệt hoặc rootkit/doorway tồn tại, sao lưu file quan trọng (nếu an toàn), sau đó cài mới hệ điều hành để đảm bảo sạch hoàn toàn.

1. Báo cáo và nhận trợ giúp chuyên nghiệp:

- Báo cáo sự cố cho cơ quan chức năng (tùy quốc gia) hoặc bộ phận an ninh mạng của công ty.

- Liên hệ chuyên gia an ninh mạng nếu dữ liệu nhạy cảm bị lộ hoặc tổn thất lớn.

## 4. Các biện pháp phòng ngừa lâu dài

• Luôn cập nhật hệ điều hành, phần mềm và trình duyệt để vá lỗ hổng bảo mật.

• Sử dụng phần mềm chống virus/anti‑malware có bản quyền và kích hoạt bảo vệ thời gian thực.

• Sao lưu định kỳ (backup) các dữ liệu quan trọng vào ổ cứng rời hoặc dịch vụ đám mây đáng tin cậy và kiểm tra khả năng khôi phục.

• Hạn chế cài phần mềm từ nguồn không rõ ràng; đọc kỹ quyền hạn khi cài ứng dụng.

• Bật xác thực hai yếu tố (2FA) cho các tài khoản quan trọng.

## Kết luận

Khi xuất hiện các dấu hiệu nêu trên, hành động nhanh chóng và hợp lí giúp giảm rủi ro mất dữ liệu hoặc lây lan. Ưu tiên cách ly thiết bị, không tương tác với mã độc, quét bằng công cụ uy tín và phục hồi từ backup nếu có. Trong trường hợp nghiêm trọng, nhờ tới chuyên gia an ninh mạng để xử lý.