**1. Ba loại phần mềm độc hại tương ứng với các dấu hiệu:**

|  |  |  |
| --- | --- | --- |
| Hiện tượng | Loại phần mềm độc hại | Giải thích |
| Máy chạy chậm bất thường, quạt kêu to | Virus hoặc Coin miner | Virus có thể chạy ngầm, chiếm tài nguyên. Coin miner bí mật dùng CPU để đào tiền ảo, gây nóng máy, quạt quay mạnh. |
| Xuất hiện nhiều cửa sổ quảng cáo lạ | Adware (phần mềm quảng cáo) | Tự động hiển thị quảng cáo khi không cần thiết; thường chèn mã quảng cáo vào trình duyệt hoặc phần mềm khác. |
| Các file bị đổi tên sang đuôi .locked | Ransomware | Ransomware mã hóa dữ liệu, đổi tên file, yêu cầu nạn nhân trả tiền chuộc để lấy lại dữ liệu. |
| Trình duyệt tự mở tab lạ | Browser hijacker hoặc adware | Thay đổi cài đặt trình duyệt, tự động mở trang web chứa quảng cáo hoặc mã độc khác. |

**2. Cách xử lý khi phát hiện các dấu hiệu nghi ngờ**

- **Ngắt kết nối Internet ngay:** Để **ngăn phần mềm độc hại tiếp tục tải xuống, lan truyền hoặc gửi dữ liệu ra ngoài** (đặc biệt nếu là ransomware hoặc keylogger).

- **Khởi động máy ở Chế độ An toàn (Safe Mode)**: Safe Mode giúp chạy máy tính với các chương trình cơ bản, dễ dàng phát hiện và gỡ bỏ phần mềm độc hại.

- **Quét toàn bộ hệ thống bằng phần mềm diệt virus uy tín:**

+ Ví dụ: **Malwarebytes, Kaspersky, Bitdefender, Windows Defender** (nếu cập nhật mới).

+ Với ransomware, thử các công cụ giải mã miễn phí từ **NoMoreRansom.org** (nếu có sẵn cho biến thể đó).

- **Sao lưu dữ liệu (nếu còn truy cập được):** Chuyển file sạch sang ổ ngoài **trước khi xử lý sâu hơn**, để tránh mất dữ liệu hoàn toàn.

- **Cân nhắc cài lại hệ điều hành**: Nếu hệ thống bị nhiễm nặng hoặc không thể gỡ sạch, **format ổ cứng và cài lại Windows** là giải pháp triệt để.