UBND TỈNH ĐẮK LẮK
SỞ GIÁO DỤC VÀ ĐÀO TẠO

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 1433/SGDĐT-QLCLCNTT
V/v triển khai cảnh báo mã độc "ValleyRAT" và tăng cường bảo đảm an toàn thông tin mạng

Đắk Lắk, ngày 10 tháng 11 năm 2025

Kính gửi: Thủ trưởng các đơn vị trực thuộc.

Thực hiện Công văn số 2340/CAT-ANM ngày 07/11/2025 của Công an tỉnh Đắk Lắk về việc cảnh báo mã độc "ValleyRAT" phát tán trên không gian mạng, Sở Giáo dục và Đào tạo (GDĐT) đề nghị các đơn vị trực thuộc khẩn trương triển khai các nội dung sau:

1. Rà soát, kiểm tra hệ thống thông tin

- Tổ chức kiểm tra toàn bộ máy tính, thiết bị lưu trữ, hệ thống mạng nội bộ tại đơn vị, đặc biệt các máy có tải hoặc chia sẻ tệp tin qua mạng xã hội (Zalo, Facebook, Telegram, Email…).

- Nếu phát hiện tập tin khả nghi như: "Dự THẢO NGHỊ QUYẾT ĐẠI HỘI.rar", "BÁO CÁO TÀI CHÍNH2.exe", "CÔNG VĂN HỎA TỐC CỦA CHÍNH PHỦ.exe", "HỖ TRỢ KÊ KHAI THUẾ.exe", "BIÊN BẢN BÁO CÁO QUÝ III.exe"… thì không được mở hoặc giải nén, đồng thời ngắt kết nối mạng (LAN/Internet) và cách ly thiết bị để xử lý.

2. Rà quét và xử lý kỹ thuật

- Thực hiện rà quét toàn bộ hệ thống bằng phần mềm diệt mã độc cập nhật mới nhất như: Windows Defender, Avast, AVG, Bitdefender (phiên bản mới).

Lưu ý: Không sử dụng Kaspersky bản miễn phí vì chưa phát hiện được mã độc ValleyRAT.

- Đối với rà quét thủ công: Kiểm tra tiến trình hoạt động trong Process Explorer, nếu phát hiện tiến trình không có chữ ký số hoặc giả mạo tên file văn bản thì nghi ngờ nhiễm mã độc. Dùng TCPView để kiểm tra kết nối mạng; nếu có kết nối đến địa chỉ IP 27.124.9.13:5689, cần ngắt kết nối ngay và báo cáo Sở GDĐT để phối hợp xử lý.

- Chặn truy cập địa chỉ IP 27.124.9.13 trên tường lửa (firewall) nội bộ của đơn vị.

3. Tuyên truyền và nâng cao cảnh giác

- Phổ biến cảnh báo này đến toàn thể cán bộ, giáo viên, nhân viên trong đơn vị, đặc biệt là người phụ trách công nghệ thông tin, văn thư, kế toán.

- Tuyệt đối không mở hoặc tải file định dạng .rar, .zip, .exe, .bat từ nguồn không xác thực hoặc chia sẻ qua mạng xã hội.

- Chỉ sử dụng tài liệu điện tử từ nguồn chính thống, có xác thực rõ ràng (từ cơ quan nhà nước, qua hệ thống thư điện tử công vụ).

- Khi nghi ngờ nhiễm mã độc, đổi ngay mật khẩu các tài khoản quan trọng (Email, Zalo, Facebook, Internet Banking, phần mềm nghiệp vụ ngành giáo dục...).

4. Trách nhiệm thực hiện

- Thủ trưởng các đơn vị trực thuộc chịu trách nhiệm chỉ đạo, tổ chức thực hiện, bảo đảm an toàn thông tin mạng trong toàn đơn vị.

- Phòng Quản lý chất lượng - Công nghệ thông tin Sở GDĐT là đầu mối tổng hợp, báo cáo lãnh đạo Sở và phối hợp với cơ quan Công an trong xử lý khi có sự cố.

Sở GDĐT yêu cầu Thủ trưởng các đơn vị trực thuộc nghiêm túc triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Lãnh đạo Sở GDĐT;
- Các phòng CMNV Sở
- Lưu: VT, QLCLCNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH ĐẮK LẮK

Lưu Tiến Quang