

**ỦY BAN NHÂN DÂN
XÃ LÂN PHONG**

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

Số: /UBND-VX

Lân Phong, ngày tháng 11 năm 2025

V/v thông báo sự cố nhiễm mã
độc và giải pháp phòng, chống

Kính gửi:

- Thường trực Đảng ủy xã;
- Thường trực HĐND xã;
- Ủy ban Mặt trận Tổ quốc Việt Nam xã và các tổ chức chính trị - xã hội xã;
- Các cơ quan chuyên trách tham mưu, giúp việc Đảng ủy xã;
- Công an xã;
- Các phòng, ban ngành xã;
- Các trường học trên địa bàn xã.

Theo nội dung Công văn số 3427/CAT-ANM ngày 03/11/2025 của Giám đốc Công an tỉnh Quảng Ngãi về việc thông báo sự cố nhiễm mã độc và giải pháp phòng, chống (*gửi đính kèm trên hệ thống quản lý văn bản và điều hành*). Công an tỉnh Quảng Ngãi đã phát hiện 02 máy tính do cán bộ UBND xã Bình Sơn đã tải 01 tập tin có tên “Dự THẢO NGHỊ QUYẾT ĐẠI HỘI.rar” từ mạng Internet. Khi mở tập tin thì máy tính bị nhiễm mã độc, chiếm quyền tài khoản Zalo, tự động gửi tập tin “Dự THẢO NGHỊ QUYẾT ĐẠI HỘI.rar” đến tất cả các nhóm, bạn bè và đăng xuất tài khoản của cán bộ này ra khỏi các nhóm Zalo để ngăn cản hoạt động thu hồi, cảnh báo về mã độc này. Vụ việc này còn xảy ra tương tự với một số đơn vị, cá nhân trên địa bàn tỉnh. Phần lớn máy tính của đơn vị bị nhiễm chưa triển khai cài đặt phần mềm phòng, chống mã độc thuộc Hệ thống phòng, chống mã độc tập trung của tỉnh Quảng Ngãi.

Mã độc trên thuộc loại Valley RAT¹, địa chỉ máy chủ điều khiển 27[.]124[.]9[.]13, port 5689. Mã độc còn phát tán với các tập tin khác: “BÁO CAO TÀI CHÍNH2.exe”; “THANH TOÁN BẢO HIỂM DOANH NGHIỆP.exe”; “CÔNG VĂN HÓA TỐC CỦA CHÍNH PHỦ.exe”; “HỖ TRỢ KÊ KHAI THUẾ.exe”; “CÔNG VĂN ĐÁNH GIÁ HOẠT ĐỘNG ĐẢNG.exe”; “MẪU GIẤY ỦY QUYỀN.exe”; “BIÊN BẢN BÁO CÁO QUÝ III.exe”. Đây mã độc có mức độ nguy hiểm rất nghiêm trọng. Tin tặc lợi dụng sự kiện Đại hội Đảng để phát tán mã độc có thể nhằm chiếm quyền điều khiển, đánh cắp, phá hoại thông tin, tài liệu nội bộ của tổ chức, cá nhân; lợi dụng làm “bàn đạp” tấn

¹ Mã độc Valley RAT là một loại Remote Access Trojan (RAT) được phát hiện đầu năm 2023, chủ yếu tấn công người dùng qua các chiến dịch phishing (lừa nạn nhân tải tài liệu miễn phí có chứa mã độc). Mục đích của ValleyRAT là giám sát và kiểm soát máy tính, hệ thống mạng máy tính bị nhiễm, từ đó tải thêm các thành phần (plugin) độc hại khác để gây hại sâu hơn. Đây là mã độc đa giai đoạn và đa thành phần, có khả năng tránh bị phát hiện bằng cách tải các thành phần theo từng giai đoạn.

công mạng các hệ thống thông tin quan trọng của cơ quan Đảng, Nhà nước hoặc thực hiện các hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội.

Với tính chất nguy hiểm nêu trên, UBND xã thông báo sự cố mã độc và giải pháp phòng, chống với những nội dung chính như sau:

1. Tổ chức rà soát từng thiết bị trong hệ thống thông tin của đơn vị; nếu có lưu trữ, kích hoạt các tệp tin mã độc nêu trên, thực hiện cô lập thiết bị, thống kê gửi thông tin về Công an xã để được hướng dẫn, hỗ trợ xử lý. Yêu cầu cán bộ, công chức, viên chức và người lao động không lưu trữ, chia sẻ, đăng tải các tệp tin mã độc này trên môi trường mạng.

2. Sử dụng các giải pháp bảo đảm an toàn thông tin mạng đã triển khai quét toàn bộ ổ đĩa thiết bị nhằm loại bỏ các mã độc đã cài đặt; bật tính năng tường lửa trên thiết bị (Windows Defender Firewall) và tiếp tục theo dõi thiết bị.

3. Triển khai các giải pháp bảo đảm an toàn thông tin theo hướng dẫn của Công an tỉnh tại Công văn số 151/CAT-ANM ngày 03/7/2025 về việc tiếp tục triển khai một số giải pháp bảo đảm an toàn thông tin mạng tỉnh Quảng Ngãi. Các trường hợp không triển khai đầy đủ các giải pháp an toàn thông tin, an ninh mạng đã được cơ quan chức năng hướng dẫn để xảy ra sự cố có hậu quả nghiêm trọng sẽ bị xử lý theo quy định pháp luật.

Quá trình thực hiện, nếu có khó khăn, vướng mắc, đề nghị liên hệ Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (*đồng chí Thượng úy Hoàng Gia Bảo, số điện thoại: 0916.401.448, email: hgbaopa05-ca@quangngai.gov.vn*).

Yêu cầu các cơ quan, đơn vị nghiêm túc triển khai thực hiện./.

Nơi nhận:

- Như trên;
- Công an tỉnh;
- CT, PCT UBND xã;
- CVP, PCVP, CVTH;
- Phòng Văn hóa – Xã hội;
- Lưu: VT.

CHỦ TỊCH

Lê Hồng Sa