BỘ CÔNG AN
**CÔNG AN TỈNH QUẢNG TRỊ**

**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM**
**Độc lập – Tự do – Hạnh phúc**

Số: 4591/CAT-PA05(Đ2)

*Quảng Trị, ngày 03 tháng 11 năm 2025*

V/v cảnh báo mã độc lan truyền trên mạng xã hội Zalo

Kính gửi:
- Các Ban Đảng, Ủy ban kiểm tra, Văn phòng Tỉnh ủy;
- Các Đảng ủy trực thuộc Tỉnh ủy;
- Văn phòng UBND tỉnh; các sở, ban, ngành, đoàn thể cấp tỉnh;
- UBND các xã, phường, đặc khu.

Qua công tác nắm tình hình, Công an tỉnh phát hiện chiến dịch lây lan mã độc nguy hiểm thông qua việc giả mạo văn bản của cơ quan nhà nước trên mạng xã hội Zalo. Các tập tin với tên gọi điển hình như: "DỰ THẢO NGHỊ QUYẾT ĐẠI HỘI.exe", "CÔNG VĂN ĐÁNH GIÁ HOẠT ĐỘNG ĐẢNG.exe". Các tập tin này khi được người dùng tải về sẽ tự động tiếp tục gửi lên các nhóm trên mạng xã hội Zalo mà người dùng có tham gia.

Qua xác minh, đây là mã độc Valley RAT, địa chỉ máy chủ điều khiển (C2): 27.124.9.13:5689, là một loại mã độc tấn công người dùng qua các chiến dịch phishing (lừa nạn nhân tải tài liệu mồi nhử có chứa mã độc). Nguy cơ khi bị lây nhiễm mã độc Valley RAT là máy tính có thể bị chiếm quyền điều khiển từ xa, theo dõi mọi hoạt động sử dụng, đánh cắp tài khoản ngân hàng, tài liệu nội bộ, dữ liệu cơ quan hoặc cài thêm các loại mã độc khác để tiến hành phá hoại sâu hơn.

Các tập tin mã độc khác có kết nối đến máy chủ điều khiển (C2) nói trên mà tin tặc có thể đã phát tán được trong thời gian gần đây gồm:

(1) BÁO CÁO TÀI CHÍNH2.exe

(2) CÔNG VĂN HỎA TỐC CỦA CHÍNH PHỦ.exe

(3) HỖ TRỢ KÊ KHAI THUẾ.exe

(4) MẪU GIẤY ỦY QUYỀN.exe

(5) BIÊN BẢN BÁO CÁO QUÝ III.exe

(6) THANH TOÁN BẢO HIỂM DOANH NGHIỆP.exe

Từ tình hình trên, để bảo đảm an toàn, an ninh mạng trên địa bàn tỉnh, Công an tỉnh - Cơ quan thường trực Tiểu ban an toàn, an ninh mạng tỉnh đề nghị các cơ quan, đơn vị, địa phương triển khai thực hiện một số nội dung sau:

**1.** Quán triệt đến cán bộ công chức, viên chức, người lao động tại đơn vị tình hình về chiến dịch lây lan mã độc, nâng cao ý thức cảnh giác về an ninh mạng, yêu cầu tuân thủ các quy định, quy chế về an ninh mạng, trong đó chú ý không mở các tập tin .exe nếu không xác minh được nguồn gửi, đặc biệt là các các tập tin có tên gọi như đã nêu ở trên.

**2.** Nhanh chóng rà soát trong hệ thống thông tin của đơn vị các tập tin nghi ngờ nói trên. Khi ghi nhận sự cố tại đơn vị, đề nghị cách ly máy tính bị nhiễm, ngắt kết nối Internet, báo cáo tình trạng cụ thể về Công an tỉnh để được hỗ trợ.

Yêu cầu Quản trị viên hệ thống thông tin tại đơn vị:

- Quét toàn bộ hệ thống bằng phần mềm bảo mật cập nhật mới nhất (EDR/XDR) có khả năng phát hiện và diệt mã độc ẩn trong bộ nhớ và các driver độc hại. Các giải pháp khuyến nghị trong trường hợp này: Avast bản free, AVG bản free, Bitdefender bản free, Windows Defender bản cập nhật mới nhất. Lưu ý: Kaspersky bản free chưa phát hiện được mã độc này.

- Trong trường hợp rà quét thủ công: (1) Kiểm tra trên Process Explorer, nếu phát hiện dấu hiệu tiến trình không có chữ ký số, xuất hiện tên tiến trình giả mạo tên tập tin văn bản. (2) Kiểm tra tcpview để xem kết nối mạng nếu phát hiện kết nối về IP máy chủ 27.124.9.13

- Khẩn trương cấu hình tường lửa, ngăn chặn truy cập đến địa chỉ IP độc hại: 27.124.9.13

**3.** Chủ quản hệ thống thông tin chủ động rà soát, chịu trách nhiệm về công tác bảo đảm an ninh mạng tại đơn vị mình. Kết quả thực hiện xin trao đổi về Công an tỉnh *(qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao)* để tập hợp chung.

Công an tỉnh đề nghị các cơ quan, đơn vị quan tâm phối hợp thực hiện./.

***Nơi nhận:***
- Thường trực Tỉnh ủy (để báo cáo);
- Ủy ban nhân dân tỉnh (để báo cáo);
- Đồng chí Giám đốc Công an tỉnh (để báo cáo);
- Như kính gửi (để phối hợp thực hiện);
- Lưu: VT, PA05(Đ2).

**KT. GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**

**Đại tá Lê Văn Hóa**