BỘ CÔNG AN
CÔNG AN TỈNH QUẢNG NGÃI

Số: 3427/CAT-ANM

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

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

Quảng Ngãi, ngày 03 tháng 11 năm 2025

HỎA TỐC

Kính gửi:
- Ủy ban Mặt trận Tổ quốc Việt Nam tỉnh;
- Văn phòng Tỉnh ủy, UBND tỉnh;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Các sở, ban ngành và hội đoàn thể tỉnh;
- Bộ Chỉ huy Quân sự tỉnh; Tòa án nhân dân tỉnh;
- Viện Kiểm sát nhân dân tỉnh; Thi hành án dân sự tỉnh;
- Bảo hiểm xã hội tỉnh; Cảng vụ Hàng hải Quảng Ngãi;
- Thống kê tỉnh; Thuế tỉnh Quảng Ngãi;
- Kho bạc Nhà nước khu vực XV;
- Báo và Phát thanh, Truyền hình Quảng Ngãi;
- Các Trường: Đại học Phạm Văn Đồng, Cao đẳng Kon Tum, Cao đẳng Việt Nam - Hàn Quốc - Quảng Ngãi;
- Công ty CP Lọc hóa dầu Bình Sơn; Truyền tải điện Quảng Ngãi; Điện lực Quảng Ngãi;
- Viettel Quảng Ngãi, VNPT Quảng Ngãi, FPT Quảng Ngãi, Mobifone Quảng Ngãi, SCTV Quảng Ngãi;
- UBND các xã, phường, Đặc khu Lý Sơn.

Qua theo dõi, giám sát an toàn thông tin, an ninh mạng trên địa bàn tỉnh, Công an tỉnh 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.

Mã độc trên thuộc loại Valley RAT[1], địa chỉ máy chủ điều khiển **27[.]124[.]9[.]13**, port 5689. Mã độc còn phát tán với các tập tin khác: "BÁO CÁO TÀI CHÍNH2.exe"; "THANH TOÁN BẢO HIỂM DOANH NGHIỆP.exe";

[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 mồi nhử 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 VĂN HỎA 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 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.

Trước tình hình trên, để bảo đảm an toàn thông tin, an ninh mạng trên địa bàn tỉnh, nhất là thời điểm diễn ra các sự kiện chính trị quan trọng của đất nước và địa phương, Giám đốc Công an tỉnh đề nghị các cơ quan, đơn vị triển khai thực hiện một số nội dung 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 tỉnh *(qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao)* 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. Các đơn vị đã được bố trí thiết bị tường lửa nhanh chóng thực hiện chặn địa chỉ IP **27[.]124[.]9[.]13** máy chủ điều khiển từ xa của mã độc.

4. 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 dung công nghệ cao *(đồng chí Thượng úy Hoàng Gia Bảo, số điện thoại: 0916.401.448, email: hgbaopa05-ca@quangngai.gov.vn).*

Đề nghị Quý cơ quan quan tâm triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Thường trực Tỉnh ủy (báo cáo);
- UBND tỉnh (báo cáo);
- Đ/c Giám đốc Công an tỉnh;
- Công an các đơn vị, địa phương;
- Lưu: VT, ANM.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đại tá Võ Văn Dương