BỘ CÔNG AN
**CÔNG AN TỈNH QUẢNG NGÃI**

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

Số: 1601/CAT-PA05

*Quảng Ngãi, ngày 01 tháng 4 năm 2024*

V/v cảnh báo máy tính của cơ quan, tổ chức và cá nhân trên địa bàn tỉnh nhiễm mã độc tống tiền

Kính gửi:
- Các tổ chức chính trị - xã hội tỉnh;
- Các sở, ban ngành, hội, đoàn thể tỉnh;
- Báo Quảng Ngãi, Đài PT - TH tỉnh Quảng Ngãi;
- UBND huyện, thị xã, thành phố;
- Truyền tải điện Quảng Ngãi;
- Công ty Điện lực Quảng Ngãi;
- Công ty Cổ phần Lọc hóa Dầu Bình Sơn;
- Các doanh nghiệp viễn thông: Viettel Quảng Ngãi, VNPT Quảng Ngãi, Mobifone Quảng Ngãi, FPT Quảng Ngãi, SCTV Quảng Ngãi.

Qua công tác bảo đảm an toàn, an ninh mạng, bảo vệ bí mật nhà nước trên không gian mạng, lực lượng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao Công an tỉnh nhận thấy nhiều trường hợp máy tính của các cơ quan, tổ chức và cá nhân trên địa bàn tỉnh nhiễm các loại mã độc tống tiền (Ransomware). Loại mã độc rất nguy hiểm, có thể dẫn đến mất dữ liệu lớn trong các cơ quan, tổ chức và cá nhân, đặc biệt khi bị nhiễm mã độc và các tài liệu đã bị mã hóa thì không thể khôi phục dữ liệu. Một số trường hợp có thể thực hiện được nhưng tốn nhiều thời gian, chi phí và không thể khôi phục lại được toàn bộ dữ liệu. Mã độc tống tiền được phát tán với nhiều phương thức tinh vi, cơ chế hoạt động mã hóa với các thuật toán mạnh mẽ, khó trong công tác giải mã:

- *Về phương thức lây lan của mã độc:* (1) Các tập tin nhiễm mã độc được gửi kèm theo thư điện tử hoặc qua ứng dụng trò chuyện trực tuyến khi người sử dụng nhận, kích hoạt tập tin sẽ làm lây nhiễm mã độc vào máy tính. (2) Các đường dẫn đến phần mềm bị giả mạo bởi mã độc được gửi qua thư điện tử, tin nhắn điện tử hoặc tồn tại trên trang thông tin điện tử không an toàn nhằm đánh lừa người sử dụng truy cập vào đường dẫn này để vô ý tự cài đặt mã độc lên máy tính. Ngoài ra máy tính còn có thể bị nhiễm thông qua các con đường khác như lây lan qua các thiết bị lưu trữ, lây qua cài đặt phần mềm...

- *Về cơ chế hoạt động:* Mã độc sau khi lây nhiễm vào máy tính sẽ tiến hành dò quét, mã hóa, đổi tên các tập tin tài liệu có đuôi mở rộng như: .doc, .docx, .pdf, .xls, .xlsx, .jpg, .zip v.v... trên tất cả các thiết bị lưu trữ có gắn vào máy tính nạn nhân và tìm cách lây lan các máy tính trong hệ thống mạng của cơ quan, tổ chức. Sau đó, mã độc sẽ yêu cầu nạn nhân thanh toán qua mạng (thẻ tín dụng hoặc tiền điện tử) để lấy được mật khẩu giải mã các tập tin đã bị

mã hóa trái phép; đe dọa sẽ công khai dữ liệu của nạn nhân nếu họ không thanh toán tiền chuộc.

Trước tình hình trên, để bảo đảm an toàn thông tin, an ninh mạng, bảo vệ dữ liệu cá nhân, dữ liệu chuyên ngành các cơ quan Đảng, Nhà nước, tổ chức, doanh nghiệp trên không gian mạng, Công an tỉnh đề nghị các cơ quan, tổ chức trên địa bàn tỉnh một số nội dung sau:

**1.** Tổ chức quán triệt, nâng cao nhận thức cho cán bộ, công chức, viên chức và người lao động về công tác phòng, chống mã độc, bảo đảm an toàn thông tin, an ninh mạng; tập trung triển khai các giải pháp sau:

- Thường xuyên cập nhật bản vá, phiên bản mới nhất cho hệ điều hành và phần mềm chống mã độc. Khuyến khích các cơ quan, tổ chức và cá nhân sử dụng các phiên bản phần mềm phòng chống mã độc có chức năng đảm bảo an toàn khi truy cập mạng Internet và phát hiện mã độc trực tuyến.

- Thường xuyên sử dụng phần mềm chống mã độc kiểm tra máy tính, ổ lưu trữ để phát hiện sớm các mã độc trên thiết bị; kiểm tra các tập tin nhận được qua thư điện tử, ứng dụng trò chuyện trực tuyến khi kích hoạt, nếu không cần thiết hoặc không rõ nguồn gốc thì không kích hoạt các tập tin này.

- Cần chú ý cảnh giác với các tập tin đính kèm, các đường dẫn được gửi đến qua thư điện tử hoặc tin nhắn điện tử, hạn chế tối đa việc truy cập vào các đường dẫn này vì tin tặc có thể đánh cắp hoặc giả mạo thư điện tử người gửi để phát tán các liên kết chứa mã độc.

- Triển khai các giải pháp kỹ thuật nhằm hạn chế quyền truy cập vào dữ liệu chỉ dành cho những người dùng cần thiết; thiết lập các cấu hình bảo vệ tập tin không cho xóa, sửa các dữ liệu quan trọng một cách tự động. Ngăn chặn thực thi ứng dụng từ các thư mục chứa dữ liệu.

**2.** Khi xảy ra vụ việc nhiễm mã độc tống tiền kịp thời phối hợp với Công an tỉnh *(qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, số điện thoại: 069.4309.485)* để được hướng dẫn xử lý, giảm thiểu hậu quả do mã độc gây ra; xác minh, điều tra, xử lý nguồn phát tán mã độc.

Đề nghị lãnh đạo các cơ quan, tổ chức quan tâm chỉ đạo thực hiện./.

***Nơi nhận:***
- Như trên;
- Thường trực Tỉnh uỷ;
- Thường trực HĐND tỉnh;
- CT, các PCT UBND tỉnh;
- Cục A05 - Bộ Công an;
- Lãnh đạo Công an tỉnh;
- Lưu: VT, PA05(Đ1).

(báo cáo)

**KT. GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**

**Đại tá Võ Văn Dương**