SỞ NÔNG NGHIỆP VÀ PTNT Q.NGÃI
CHI CỤC KIỂM LÂM

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

Số: 315 /CCKL-TCHC

V/v cảnh báo máy tính nhiễm mã độc tống tiền

Quảng Ngãi, ngày 04tháng 4 năm 2024

Kính gửi: Các phòng, Đội KLCĐ, Hạt kiểm lâm các huyện

Theo Công văn số 1297/SNNPTNT-VP ngày 02/4/2024 của Sở Nông nghiệp và phát triển nông thôn về việc cảnh báo máy tính của các cơ quan, tổ chức và cá nhân trên địa bàn tỉnh nhiễm mã độc tống tiền;

Nhằm đảm bảo an toàn thông tin, an ninh mạng, bảo vệ dữ liệu cá nhân, dữ liệu Chi cục trưởng Chi cục Kiểm lâm yêu cầu Trưởng các phòng chuyên môn, Đội, Hạt kiểm lâm các huyện triển khai thực hiện một số nội dung sau:

1. Quán triệt, thông tin kịp thời đến toàn thể công chức, viên chức, người lao động tại cơ quan, đơn vị về mã độc tống tiền (Ransomware) để nâng cao nhận thức về công tác phòng, chống mã độc, bảo đảm an toàn thông tin, an ninh mạng, cụ thể:

- Loại mã độc này rất nguy hiểm, có thể dẫn đến mất dữ liệu; khi bị nhiễm mã độc và các tài liệu đã bị mã hóa thì không thể khôi phục dữ liệu.

- Về phương thức lây lan của mã độc: Các tập tin nhiễm mã độc được gửi kèm theo thư điện tử hoặc qua ứng dụng trò chuyện trực tuyến khi người dùng nhận, kích hoạt tập tin sẽ làm lây nhiễm mã độc vào máy tính. 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 tiền 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.

2. Kịp thời chỉ đạo công chức, viên chức, người lao động tại cơ quan, đơn vị 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 phòng chuyên môn, Đội, Hạt kiểm lâm các huyện 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.

3. 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.

Yêu cầu Trưởng các phòng chuyên môn, Đội, Hạt kiểm lâm các huyện triển khai thực hiện.

Nơi nhận:
- Như trên;
- Sở NN và PTNT (b/c)
- Lãnh đạo Chi cục;
- Lưu: VT, TCHC (b.ngọc).

CHI CỤC TRƯỞNG

Phạm Duy Hưng