THANH TRA TỈNH **VĂN PHÒNG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 4 / TB-VP V/v cảnh báo hình thức lây nhiễm mới của mã độc thuộc loại Ransomware mã hóa dữ liệu tống tiền.	*Tây Ninh, ngày 7 tháng 04 năm 2016*

Kính gửi:
- Ban lãnh đạo Thanh tra;
- Văn phòng, các phòng Nghiệp vụ;

Thực hiện Công văn số 145/STTTT-TTCNTT ngày 18 tháng 3 năm 2016 của Sở Thông tin và Truyền thông tỉnh Tây Ninh về việc cảnh báo hình thức lây nhiễm mới của mã độc thuộc loại Ransomware mã hóa dữ liệu tống tiền.

Hiện nay, tình trạng lây nhiễm mã độc này **đặc biệt nghiêm trọng** và đang lây lan nhanh chóng, ***hiện đã có một số máy tính của Sở, ngành ở tỉnh bị lây nhiễm mà độc này gửi qua hệ thống email***. Để phòng ngừa các loại mã độc Ransomware, Văn phòng Thanh tra tỉnh thông báo, khuyến cáo thông tin và cách phòng trách hạn chế bị nhiễm mã độc như sau:

1. Chú ý phòng ngừa để hạn chế tối đa khả năng bị nhiễm mã độc:

- Người sử dụng thư điện tử có thể nhận các thư điện tử chứa virus từ các địa chỉ giả mạo như;

Các thư điện tử có tiêu đề có chứa chữ " Emailing: "

Các tập tin đính kèm có đuôi như :IMAGE.JPEG, SCAN.DOCX, SHEET.TILL,.ZIP,.DOC, PDF, JS, XLS...

Các địa chỉ giả mạo như:

EPSON@tayninh.gov.vn,COPIER@tayninh.gov.vn, CANON@tayninh .gov.vn....

Tên cơ quan đơn vị nhà nước ví dụ: *tencoquan@tayninh.gov.vn*.

- Thiết bị lưu trữ USB, đĩa CD và DVD bắt buộc phải quét vi rút trước khi đưa vào sử dụng.

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

- Sử dụng phần mềm diệt virus kiểm tra các tập tin được gửi qua thư điện tử, tải từ trên mạng về trước khi kích hoạt. Nếu không cần thiết hoặc không rõ nguồn gốc thì không kích hoạt các tập tin này.

- Thường xuyên cập nhật bản vá, phiên bản mới nhất phần mềm chống mã độc (Kaspersky, Synmatec, Avast, Avira, AVG, BKAV.....).

- Tắt chế độ tự động mở, chạy các tập tin (autoruns) đính kèm theo thư điện tử.

2. Thực hiện sao lưu định kỳ dữ liệu

- Cần tiến hành sao lưu dữ liệu định kỳ, thường xuyên để có thể khôi phục dữ liệu khi máy tính bị Ransomware gây hại.

3. Xử lý khi phát hiện bị lây nhiễm mã độc

Khi mã độc Ransomware lây nhiễm vào máy tính bị hại, mã độc sẽ tiến hành mã hóa các tập tin dữ liệu trong một khoản thời gian, đồng thời khóa máy tính của người dùng để người dùng không can thiệp tắt các tiến trình đang chạy. Do đó, việc phản ứng nhanh chóng khi phát hiện ra sự cố có thể giúp giảm thiểu thiệt hại cho các dữ liệu chứa trên máy bị nhiễm và tăng khả năng khôi phục các dữ liệu đã bị mã hóa. Cụ thể, đối với các máy tính cá nhân khi phát hiện có dấu hiệu bị nhiễm mã độc Ransomware cần phải nhanh chóng thực hiện các thao tác sau:

- Nhanh chóng tắt máy tính bằng cách ngắt ngay nguồn điện (không sử dụng chức năng shutdown của Hệ điều hành Windows). Cách ly máy tính ra khỏi mạng nội bộ nhằm ngăn ngừa trường hợp có thể lây nhiễm sang các máy tính khác trong hệ thống.

- Không được tự ý khởi động lại máy tính. Phải báo ngay cho bộ phận chuyên trách Công nghệ thông tin để có hướng xử lý./.

Nơi nhận:
- Như trên;
- Lưu VT. (M.An)

KT.CHÁNH THANH TRA
PHÓ CHÁNH THANH TRA

Digitally signed by
Trần Văn Cẩn
Thanh tra tỉnh
Tỉnh Tây Ninh
Tây Ninh, VN
Date: 7.4.2016 13:50