UBND TỈNH AN GIANG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 49 /STTTT-CNTT
V/v Hướng dẫn thực hiện các biện pháp phòng ngừa mã độc RanSomware

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

An Giang, ngày 13 tháng 02 năm 2015

Kính gửi:
- Các Sở, Ban, Ngành cấp tỉnh;
- UBND các huyện, thị, thành phố;
- Các cơ quan Đảng, Đoàn thể;
- Hiệp Hội doanh nghiệp.

Trên cơ sở Công văn số 21/VNCERT-NV ngày 06 tháng 02 năm 2015 của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) về cảnh báo mã độc thuộc loại RanSomware mã hoá dữ liệu để tống tiền,

Theo đó, đây là loại mã độc rất nguy hiểm có thể dẫn đến mất mát dữ liệu lớn trong các cơ quan, tổ chức và cá nhân. Đặc biệt, khi bị nhiễm mã độc các tài liệu bị mã hoá thì không thể khôi phục dữ liệu. Một số trường hợp có thể thực hiện được nhưng mất nhiều thời gian và chi phí, nhưng không thể khôi phục được toàn bộ dữ liệu. Do tình hình lây lan hiện nay rất phức tạp, đề nghị các cơ quan, tổ chức cần chú ý và tăng cường công tác phòng ngừa sự cố có thể xảy ra.

Loại mã độc trên lây lan chủ yếu qua hai phương pháp là:

- Gửi tệp tin nhiễm mã độc kèm theo thư điện tử, khi người sử dụng kích hoạt tệp tin đính kèm thư điện tử sẽ làm lây nhiễm mã độc vào máy tính.

- Gửi thư điện tử hoặc tin nhắn điện tử có chứa đường dẫn đến phần mềm bị giả mạo bởi mã độc Ransomware và 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 đường khác như: lây lan qua các thiết bị lưu trữ, lây qua cài đặt phần mềm, sao chép dữ liệu, phần mềm...

Mã độc Ransomware sau khi lây nhiễm vào máy tính người bị hại, sẽ dò quét các tệp 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 của máy nạn nhân và tự động mã hóa và đổi tên các tệp tin đó bằng cách sử dụng thuật toán mã hóa với khóa công khai, một số loại mã độc còn tiến hành khóa máy tính nạn nhân không cho sử dụng. Sau đó mã độc sẽ yêu cầu người bị hại thanh toán qua mạng (thẻ tín dụng, hoặc bitcoin) để lấy được mật khẩu giải mã các tệp tin đã bị mã hóa trái phép. Hiện nay vẫn chưa có phần mềm hoặc dịch vụ thương mại nào cho phép giải mã các tệp tin đã bị mã độc Ransomware, nếu không lấy được mật khẩu giải mã của tin tặc phát tán mã độc.

Để phòng ngừa các loại mã độc Ransomware trong tình hình hiện nay, Sở Thông tin và Truyền thông hướng dẫn các cơ quan, đơn vị trên địa bàn tỉnh An Giang thực hiện một số biện pháp sau:

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

- Thường xuyên cập nhật bản vá, phiên bản mới nhất cho hệ điều hành và phần mềm chống mã độc (Kaspersky, Synmatec, Avast, AVG, MSE, Bkav, CMC, v.v...).

- Thường xuyên sử dụng phần mềm diệt mã độc, virus kiểm tra máy tính, ổ lưu trữ để phát hiện sớm nếu xuất hiện mã độc trên thiết bị.

- Cần chú ý cảnh giác với các tệp 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 người gửi phát tán các kết nối chứa mã độc.

- Sử dụng phần mềm diệt virus kiểm tra các tệp 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 tệp tin này.

- Các đơn vị, cá nhân khi nhận được các email nghi vấn nhiễm mã độc, không kích hoạt mở thư điện tử, không thực hiện việc chuyển tiếp thư đó qua các địa chỉ email khác để tránh trường hợp gây nhiễm hoặc phát tán cho các địa chỉ nhận;

- Tắt chế độ tự động mở, chạy các tệp tin đính kèm theo thư điện tử.

2. Thực hiện sao lưu định kỳ dữ liệu

Cần tiến hành sao lưu định kỳ dữ liệu thường xuyên để có thể khôi phục dữ liệu khi máy tính bị Ransomware gây hại, các cơ quan, tổ chức có thể tham khảo một số biện pháp sau:

- Sử dụng đĩa CD ROM, DVD ROM để sao lưu dữ liệu là phương pháp đơn giản và an toàn, tuy nhiên không được thuận tiện khi sử dụng lâu dài và thường xuyên.

- Sử dụng các ổ lưu trữ USB, ổ đĩa cắm ngoài, ổ chia sẻ mạng v.v... Cần chú ý dữ liệu trong các ổ lưu trữ này hoàn toàn có thể bị ảnh hưởng nếu kết nối vào máy tính đã bị nhiễm mã độc Ransomware. Do vậy phải đảm bảo máy chưa bị nhiễm mã độc trước khi sao lưu hoặc khởi động máy tính từ ổ đĩa khởi động ngoài khi thực hiện sao lưu để đảm bảo an toàn.

Sử dụng các công cụ, giải pháp chuyên dụng để sao lưu như: các máy chủ quản lý tệp tin, máy chủ sao lưu từ xa, các công cụ lưu trữ đám mây cho phép khôi phục lịch sử thay đổi của tập tin mà khi xảy ra sự cố có thể khôi phục lại từ thời điểm trước đó...

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 tệp tin dữ liệu, khóa máy tính của người dùng để người dùng không can thiệp để tắt tiến trình đang chạy. Do đó, việc phản ứng nhanh chóng khi phát hiện sự cố có thể giúp giảm thiểu thiệt hại cho các dữ liệu chứa trên máy tính bị nhiễm và giúp các chuyên gia có thể khôi phục các dữ liệu bị mã hóa. Cụ thể, đối với các máy tính cá nhân khi phát hiện ra dấu hiệu bị lây nhiễm mã độc Ransomware cần phải nhanh chóng thực hiện các thao tác sau:

- Nhanh chóng tắt máy tính (Tắt nguồn điện, không sử dụng chức năng shutdown của hệ điều hành).

- Mặc dù không có khả năng giải mã các tệp tin đã bị mã độc mã hóa, nhưng trong một số trường hợp có thể sử dụng các phần mềm khôi phục dữ liệu (FTK, EaseUs, R-STUDIO) để khôi phục các tệp tin nguyên bản đã bị xóa. Do vậy, nếu không có kinh nghiệm xử lý sự cố này cần yêu cầu sự hỗ trợ sớm của các chuyên gia an toàn thông tin để giảm thiểu các thiệt hại khi xảy ra sự cố.

- Phải sử dụng khởi động từ hệ thống sạch (từ ổ đĩa CD/DVD hay USB) hoặc tháo ổ cứng ra để kết nối vào máy tính sạch khác. Sau đó thực hiện kiểm tra các tệp dữ liệu và sao lưu các dữ liệu chưa bị mã hóa.

- Cài đặt lại toàn bộ hệ thống, cài phần mềm diệt virus cập nhật phiên bản mới nhất và tiến hành quét toàn bộ dữ liệu trên máy tính trước khi sao chép lại các dữ liệu vào máy tính.

Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị nâng cao cảnh giác, kịp thời phòng tránh và có biện pháp khắc phục.

Đề nghị các đơn vị chủ động và phối hợp cùng Sở Thông tin và Truyền thông, thực hiện các biện pháp phòng ngừa mã độc theo hướng dẫn. Trong quá trình thực hiện nếu có khó khăn vướng mắc vui lòng liên hệ Trung tâm Tin học – Sở Thông tin và Truyền thông qua địa chỉ hotro@angiang.gov.vn hoặc thông báo về số điện thoại 0763.954.166.

Trân trọng kính chào./.

Nơi nhận:
- Như trên;
- SoTTTT: BGĐ; TTTH, TTDVCNTT&TT, P.CNTT;
- Lưu: VT.

(Kèm CV 21/VNCERT-NV ngày 06/02/2015)

GIÁM ĐỐC

Ký bởi: Sở Thông tin và Truyền thông
Email: sotttt@angiang.gov.vn
Cơ quan: Tỉnh An Giang
Thời gian ký: 13.02.2015 14:51:46 +07:00

Trương Minh Thuần