BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

Số: 21 /VNCERT-NV

V/v cảnh báo mã độc thuộc loại Ransomware mã hoá dữ liệu để tống tiền

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

Hà Nội, ngày 06 tháng 02 năm 2015

Kính gửi:

- Các Sở Thông tin và Truyền thông
- Các đơn vị chuyên trách về CNTT các Bộ, Ngành
- Các thành viên mạng lưới ứng cứu sự cố Internet Việt Nam.

Đầu tháng 01/2014 thông qua phương tiện truyền thông (Báo ICTNews), Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) đã đưa ra cảnh báo tới người dùng Internet về việc xuất hiện sự xuất hiện và lây lan của mã độc mã hoá dữ liệu Ransomware trên hệ điều hành Microsoft Windows tại Việt Nam. Trong tháng 01/2015 và đặc biệt thời gian gần đây, Trung tâm VNCERT nhận được nhiều thông tin phản ánh về việc lây nhiễm các phiên bản mới của mã độc Ransomware như CTB Locker/Critroni hoặc Onion trong nhiều cơ quan tổ chức tại Việt Nam. Trung tâm VNCERT nhận thấy 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 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 và chi phí và không thể khôi phục lại 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.

Hai phương pháp lây lan chủ yếu của mã độc Ransomware 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 con 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 trên 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, Trung tâm VNCERT khuyến cáo các đơn vị thực hiện một số biện pháp sau:

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

- Thiết lập quyền người sử dụng không ở chế độ quản trị hệ thống (admin) và thiết lập các cấu hình bảo vệ tệp tin không cho xóa, sửa các tệp dữ liệu quan trọng một cách tự động. Ngăn chặn thực thi ứng dụng từ các thư mục chứa dữ liệu.

- 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...). Khuyến khích các cơ quan, tổ chức 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 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.

- 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 trong một khoảng thời gian đồng thời 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 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 bị mã hóa. Cụ thể là đối với các máy tính cá nhân khi phát hiện có dấu hiệu bị lây nhiễm mã độc Ransomware cần phải nhanh chóng thực hiện các thao tác sau:

- Nhanh chóng tắt máy tính bằng cách ngắt nguồn điện (chức năng shutdown của hệ điều hành Windows đã bị chặn không còn tác dụng).

- Không được khởi động lại máy tính theo cách thông thường mà phải khởi động lại máy tính từ hệ điều hành 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.

- Các tệp tin đã bị mã hóa hầu như không thể giải mã được 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.

- Cài đặt lại toàn bộ hệ thống, cài phần mềm diệt virus cập nhật phiên bản mới nhất và tiến hành quét kiểm tra mã độc toàn bộ máy tính trước khi sao chép trả lại các dữ liệu an toàn đã sao lưu vào máy tính.

Để giúp các cơ quan chức năng theo dõi, phân tích và phản ứng nhanh chóng với các loại mã độc mới, ngay khi phát hiện xảy ra sự cố về mã độc Ransomware cần nhanh chóng thông báo về đầu mối ứng cứu sự cố của VNCERT. Thông tin đầu mối tiếp nhận sự cố: Phòng Nghiệp vụ - Trung tâm VNCERT, số điện thoại: 0934424009/0436404421 hoặc qua email: ir@vncert.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Bộ trưởng Nguyễn Bắc Son (để b/c)
- Thứ trưởng Nguyễn Minh Hồng (để b/c)
- Cục ATTT (để phối hợp)
- Lưu: VT, KTHT, NV.

GIÁM ĐỐC

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

Vũ Quốc Khánh