BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM
Số: 80 /VNCERT-ĐPUC

Cảnh báo hình thức lây nhiễm mới của mã độc mã hoá tài liệu (Ransomware)

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

Hà Nội, ngày 09 tháng 03 năm 2016

Kính gửi:

- Các đơn vị chuyên trách về CNTT các Bộ, Ngành;
- Các Sở Thông tin và Truyền thông;
- Các nhà cung cấp dịch vụ Internet (ISP);
- Các đơn vị thuộc Bộ Thông tin và Truyền thông

Trong tuần đầu tháng 03/2016, Trung tâm VNCERT ghi nhận cách thức tấn công mới của tin tặc nhằm vào các cơ quan tổ chức có sử dụng các hòm thư điện tử nội bộ. Với cách tấn công mới này, tin tặc sẽ giả mạo một địa chỉ điện tử có đuôi là @tencongty.com.vn để gửi thư điện tử có kèm mã độc đến các người dùng trong công ty đó. Để qua mặt các hệ thống dò quét mã độc, các mã độc thường được nén lại dưới định dạng .zip hoặc .zar. Qua phân tích của chuyên gia VNCERT với một sự cố cho thấy, tệp tin chứa mã độc .zip chứa bên trong các tệp tin thực thi như **.js** (đây là một tệp tin Javascript) hoặc tệp tin văn bản như **.doc**, **.xls...**, khi người dùng mở tập tin này mã độc sẽ được kích hoạt và tự động tải tập tin mã độc mã hóa tài liệu và tự thực thi trên máy. Với trường hợp mã độc mã hóa tài liệu thì mã độc sẽ tiến hành mã hoá nội dung toàn bộ các dữ liệu trên máy nạn nhân với thuật toán mã hóa mạnh để không thể giải mã được với mục đích bắt cóc dữ liệu trên máy để tống tiền nạn nhân. Với việc giả mạo chính các địa chỉ thư điện tử của đơn vị sẽ làm cho người dùng khó phát hiện các thư giả mạo dẫn đến số lượng các máy tính bị lây nhiễm mã độc mã hóa dữ liệu có thể tăng cao.

Thực hiện Thông tư số 27/2011/TT-BTTTT ngày 04/10/2011 của Bộ Thông tin và Truyền thông quy định về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam, nhằm ngăn chặn sự lây lan và giảm thiểu thiệt hại cho người dùng Internet, Trung tâm VNCERT yêu cầu các cơ quan, tổ chức cần chú ý và tăng cường công tác tuyên truyền rộng rãi đến các nhân viên, người dùng máy tính để phòng ngừa sự cố có thể xảy ra.

Các phương pháp lây lan chủ yếu của mã độc mã hoá tài liệu là:

1. Gửi tập tin đính kèm thư điện tử, khi người dùng mở tập tin thì mã độc sẽ tự động lây nhiễm vào máy tính người dùng;

2. Gửi thư điện tử hoặc tin nhắn điện tử có chứa đường dẫn đến mã độc và yêu cầu người dùng tải về và cài đặt;

Ngoài ra máy tính còn có thể bị lây nhiễm thông qua đường khác như qua các thiết bị lưu trữ, qua quá trình cài đặt phần mềm không rõ nguồn gốc, sao chép dữ liệu từ máy nhiễm,...

Dấu hiệu nhận biết của loại mã độc sau khi máy tính bị nhiễm là các tài liệu, văn bản sẽ bị thay đổi nội dung và đổi tên phần mở rộng, phổ biến là các tập tin có định dạng: .doc, .docx, .pdf, .xls, .xlsx, .jpg, .txt, .ppt, .pptx,...một số loại còn khoá máy tính không cho sử dụng và đòi tiền chuộc.

Để phòng ngừa các loại mã độc Ransomware trong tình hình hiện nay, Trung tâm VNCERT khuyến cáo các đơn vị xử lý một số biện pháp sau:

1. Phòng ngừa để hạn chế tối đa khả năng bị nhiễm mã độc:

- Phân quyền hợp lý cho các loại tài khoản người dùng, bảo vệ các tập tin không cho phép xoá, sửa nội dung các tập tin quan trọng.

- Cài đặt và thường xuyên cập nhật cho hệ điều hành, phần mềm chống mã độc như Kaspersky, Symantec, Avast, AVG, MSE, Bkav, CMC,...

- Chú ý cảnh giác với các tập tin đính kèm, các đường liên kết ẩn được gửi đến thư điện tử người dùng, kể cả người gửi từ trong nội bộ.

- Thực hiện các biện pháp kỹ thuật nhằm kiểm tra xác thực người dùng trên máy chủ gửi email của đơn vị, tránh bị giả mạo người gửi từ nội bộ.

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

2. Thực hiện sao lưu dữ liệu định kỳ:

- Sử dụng các ổ đĩa lưu trữ như Ổ cứng cắm ngoài, Ổ đĩa USB để lưu trữ các dữ liệu quan trọng trong máy tính. Sau khi sao lưu xong đưa ra cất giữ riêng.

- Sử dụng các công cụ, giải pháp chuyên dụng để sao lưu dữ liệu như: các máy chủ quản lý tập 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.

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

Khi mã độc lây nhiễm vào máy tính, mã độc sẽ tiến hành quét và mã hoá các tập tin trong một khoảng thời gian. Do đó, việc phản ứng nhanh khi phát hiện ra sự cố có thể giúp giảm thiểu thiệt hại cho dữ liệu trên máy tính và tăng khả năng khôi phục dữ liệu bị mã hoá. Cụ thể cần thực hiện các thao tác sau:

- Nhanh chóng tắt máy tính bằng các ngắt nguồn điện.

- Không được khởi động lại máy tính theo cách thông thường mà phải khởi động từ hệ điều hành sạch khác (khuyến nghị hệ điều hành Linux) như từ ổ đĩa CD, USB,...sau đó thực hiện kiểm tra các tập tin dữ liệu và sao lưu các dữ liệu chưa bị mã hoá.

- Các tập tin đã bị mã hoá tương đối khó để giải mã, tuy nhiên trong một số trường hợp có thể sử dụng các phần mềm khôi phục dữ liệu như FTK, EaseUs, R-STUDIO,...để khôi phục các tập tin nguyên bản đã bị xoá.

- Cài đặt lại toàn bộ hệ thống, cài đặt phần mềm diệt virus đồng thời thiết lập chế độ cập nhật phiên bản tự động.

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 điều phối ứng cứu quốc gia:

Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT)

- Địa chỉ: 18 Nguyễn Du – Hai Bà Trưng – Hà Nội
- Điện thoại: 0436404423
- Điện thoại di động: 0934424009
- Hòm thư điện tử tiếp nhận sự cố: ir@vncert.gov.vn

Trân trọng cảm ơn./.

Nơi nhận:
- Như trên;
- Bộ Trưởng Nguyễn Bắc Son (để b/c);
- Thứ Trưởng Nguyễn Thành Hưng (để b/c);
- Cục An toàn thông tin;
- Giám đốc (để b/c);
- Chi nhánh Hồ Chí Minh;
- Chi nhánh Đà Nẵng;
- Lưu: VT, ĐPƯC (01), KTHT (01).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

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

Nguyễn Khắc Lịch