ỦY BAN NHÂN DÂN THỊ XÃ AN KHÊ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 95 /UBND – VP Về việc cảnh báo mã độc mã hóa dữ liệu trên máy tính để tống tiền.	*An Khê, ngày 10 tháng 3 năm 2015*

Kính gửi:

- Thủ trưởng các cơ quan thuộc thị xã;
- Ủy ban nhân dân các xã, phường.

Ủy ban nhân dân thị xã An Khê nhận được công văn số 81/STTTT-CNTT ngày 25/02/2015 của Sở Thông tin Truyền thông về việc cảnh báo mã độc thuộc loại Ransomware mã hóa dữ liệu để tống tiền.

Để kịp thời cảnh báo, phát hiện và ngăn chặn nguy cơ mất an toàn thông tin từ loại mã độc này, Ủy ban nhân dân thị xã An Khê thông báo đến các cơ quan, đơn vị trên địa bàn thị xã nghiên cứu nội dung công văn số 21/VNCERT-NV ngày 06/02/2015 của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam thuộc Bộ Thông tin và Truyền thông (*gửi kèm theo*), tổ chức thực hiện các giải pháp, phòng chống loại mã độc này theo hướng dẫn.

Đề nghị Thủ trưởng các cơ quan, ban ngành trên địa bàn, Ủy ban nhân dân các xã, phường quan tâm thực hiện./.

Nơi nhận:
- Như trên;
- Lưu VT.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Hùng Vỹ

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