BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG
CỤC CÔNG NGHỆ THÔNG TIN

Số: 211/CNTT-CSHT
V/v: Cảnh báo nguy cơ mất an toàn dữ liệu từ mã độc máy tính

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

Hà Nội, ngày 25 tháng 5 năm 2015

Kính gửi:
- Các đơn vị trực thuộc Bộ Tài nguyên và Môi trường;
- Các Sở Tài nguyên và Môi trường.

Trong thời gian gần đây trên môi trường internet xuất hiện một loại mã độc lây nhiễm vào các máy tính nhằm mã hóa toàn bộ các file dữ liệu người dùng và đưa ra các yêu cầu tống tiền người dùng nếu muốn cứu lại dữ liệu của mình với nhiều biến thể ngày càng nguy hiểm và tinh vi hơn.

Trong quá trình theo dõi giám sát các hoạt động đảm bảo an toàn cho hệ thống mạng thông tin ngành Tài nguyên và môi trường. Chúng tôi nhận thấy có nhiều máy tính trong các đơn vị ngành Tài nguyên và môi trường đã bị lây nhiễm loại mã độc trên và hệ thống mạng máy tính tại các đơn vị trong ngành có nguy cơ cao dễ bị lây nhiễm các loại biến thể của loại mã độc này.

Đặc điểm của loại mã độc này là được phát toán thông qua thư điện tử rác (spam mail), từ các trang web, mạng xã hội, chia sẻ dữ liệu qua mạng LAN, qua các thiết bị lưu trữ như usb, thẻ nhớ… Mã độc sẽ được kích hoạt sau khi người dùng nhấp tải file đính kèm và thực hiện công việc như kiểm soát máy tính, mã hóa các file dữ liệu (Word, Excel, …).

Khi bị lây nhiễm, dữ liệu đã bị mã hóa sẽ không thể được khôi phục vì hacker sử dụng thuật mã hóa công khai và khóa bí mật dùng để giải mã chỉ được lưu giữ trên máy chủ của hacker. Ngoài ra, trên các máy tính cá nhân bị nhiễm mã độc, nhiều nạn nhân còn nhận được thông điệp đòi tiền chuộc của hacker nhằm giải mã những dữ liệu đã bị kiểm soát.

Cụ thể, nạn nhân sẽ nhận được thông báo phải nộp tiền chuộc trong vòng một khoảng thời gian nhất định nào đó, nếu không file sẽ bị mã hóa vĩnh viễn.

Trước tình hình trên, Cục Công nghệ thông tin kính đề nghị các đơn vị, cá nhân cần phổ biến và thực hiện ngay một số khuyến nghị nhằm đảm bảo an toàn dữ liệu sau:

- Không nên mở file đính kèm từ các email không rõ nguồn gốc đặc biệt là các tệp tin đính kèm đuôi zip, rar;
- Cài đặt và cập nhật thường xuyên phần mềm diệt virus trên các máy PC để phòng tránh, ngăn chặn các virus lây lan trên máy tính, hệ thống mạng;
- Diệt virus cho USB khi cắm USB vào máy tính;
- Không nên truy cập vào những trang Web, các đường link, tải những file không rõ nguồn gốc trên mạng;
- Sao lưu dữ liệu thường xuyên để có thể khôi phục lại khi dữ liệu bị mất hoặc bị mã hóa.

Đề nghị Quý cơ quan, đơn vị nhanh chóng kiểm tra, rà soát hệ thống máy tính và thực hiện ngay một số khuyến nghị trên. Nếu Quý cơ quan bị lây nhiễm mã độc này, đề nghị thông báo trực tiếp về Cục Công nghệ thông tin thông qua Trung tâm Cơ sở hạ tầng công nghệ thông tin để nắm tình hình và có biện pháp hỗ trợ nếu cần thiết. Mọi thông tin chi tiết xin liên hệ anh Lê Minh Quang, Trưởng phòng An toàn thông tin số và xử lý sự cố theo số điện thoại 04 62542057, hòm thư điện tử citi@tnmt.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Nguyễn Linh Ngọc (để b/c);
- Lưu VT.

CỤC TRƯỞNG

CỘNG HOÀ X.H.C.N VIỆT NAM
CỤC CÔNG NGHỆ THÔNG TIN
BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG

Nguyễn Hữu Chính