UBND TỈNH BÌNH ĐỊNH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 331/STTTT-CNTT
V/v cảnh báo mã độc tấn công đòi tiền chuộc

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

Bình Định, ngày 15 tháng 5 năm 2017

Kính gửi:
- Các sở, ban, ngành;
- UBND các huyện, thị xã, thành phố.

Theo cảnh báo từ Cục An toàn thông tin, Bộ Thông tin và Truyền thông, hiện tại, mã độc có tên là WannaCry khai thác một số lỗ hổng trên hệ điều hành Windows để tấn công vào các máy tính với mục tiêu mã hóa dữ liệu để đòi tiền chuộc, ảnh hưởng tới nhiều tổ chức, cá nhân trên phạm vi toàn cầu. Trước nguy cơ bị mã độc ransomware WannaCry tấn công, mã hóa dữ liệu quan trọng để đòi tiền chuộc, Sở Thông tin và Truyền thông yêu cầu các cơ quan, địa phương trên địa bàn tỉnh cần thực hiện ngay các biện pháp phòng tránh như sau:

1. Đối với cá nhân

- Thực hiện cập nhật ngay các phiên bản hệ điều hành Windows đang sử dụng. Riêng đối với các máy tính sử dụng Windows XP, sử dụng bản cập nhật mới nhất dành riêng cho sự vụ này tại: https://www.microsoft.com/en-us/download/details.aspx?id=55245&WT.mc_id=rss_windows_allproducts hoặc tìm kiếm theo từ khóa bản cập nhật KB4012598 trên trang chủ của Microsoft.

- Cập nhật ngay các chương trình Antivius đang sử dụng. Đối với các máy tính không có phần mềm Antivirus cần tiến hành cài đặt và sử dụng ngay một phần mềm Antivirus có bản quyền.

- Cẩn trọng khi nhận được email có đính kèm và các đường link lạ được gửi trong email, trên các mạng xã hội, công cụ chat…

- Cần thận trọng khi mở các file đính kèm ngay cả khi nhận được từ những địa chỉ quen thuộc. Sử dụng các công cụ kiểm tra phần mềm độc hại trực tuyến hoặc có bản quyền trên máy tính với các file này trước khi mở ra.

- Không mở các đường dẫn có đuôi .hta hoặc đường dẫn có cấu trúc không rõ ràng, các đường dẫn rút gọn link.

- Thực hiện biện pháp lưu trữ (backup) dữ liệu quan trọng ngay.

2. Đối với cơ quan, địa phương (cụ thể với các quản trị mạng)

- Kiểm tra ngay lập tức các máy chủ và tạm thời khóa (block) các dịch vụ đang sử dụng các cổng 445/137/138/139.

- Tiến hành các biện pháp cập nhật sớm, phù hợp theo từng đặc thù cho các máy chủ windows của cơ quan, địa phương. Tạo các bản snapshot đối với các máy chủ ảo hóa đề phòng việc bị tấn công.

- Có biện pháp cập nhật các máy trạm đang sử dụng hệ điều hành Windows.

- Cập nhật cơ sở dữ liệu cho các máy chủ Antivirus Endpoint đang sử dụng. Đối với hệ thống chưa sử dụng các công cụ này thì cần triển khai sử dụng các phần mềm Endpoint có bản quyền và cập nhật mới nhất ngay cho các máy trạm.

- Tận dụng các giải pháp đảm bảo an toàn thông tin đang có sẵn trong cơ quan, như Firewall, IDS/IPS, SIEM.. để theo dõi, giám sát và bảo vệ hệ thống trong thời điểm nhạy cảm này. Cập nhật các bản cập nhật từ các hãng bảo mật đối với các giải pháp đang có sẵn. Thực hiện ngăn chặn, theo dõi domains đang được mã độc WannaCry sử dụng là: http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/

- Cân nhắc việc ngăn chặn (block) việc sử dụng Tor trong cơ quan.

- Thực hiện biện pháp lưu trữ (backup) dữ liệu quan trọng ngay.

- Cảnh báo tới người dùng trong cơ quan và thực hiện các biện pháp như nêu trên đối với người dùng.

Trong quá trình thực hiện, nếu có vướng mắc, đề nghị các cơ quan liên hệ trực tiếp Sở Thông tin và Truyền thông gặp đ/c Ngô Duy Trung, số điện thoại: 0905.221.417 hoặc đ/c Lê Quốc Việt, số điện thoại: 0916.494.679 để được hướng dẫn cụ thể./.

Nơi nhận:
- Như trên;
- Giám đốc Sở (b/c);
- Trung tâm CNTT và TT;
- Lưu: VT, CNTT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH BÌNH ĐỊNH

Võ Gia Nghĩa