UBND TỈNH KIÊN GIANG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số : 247/STTTT-CNTT
V/v cảnh báo và khuyến nghị đến các cơ quan nhà nước người dân, doanh nghiệp và các tổ chức về tình hình mã độc tấn công các hệ thống thông tin

Kiên Giang, ngày 15 tháng 5 năm 2017

KHẨN

Kính gửi:
- Văn phòng Ủy ban nhân dân tỉnh;
- Các sở, ban, ngành tỉnh;
- Ủy ban nhân dân các huyện, thị xã, thành phố.

Vừa qua, mã độc máy tính có tên WannaCry khai thác một số lỗ hổng trên hệ điều hành Windows (hệ điều hành máy tính phổ biến nhất hiện nay) để tấn công vào các máy tính với mục tiêu mã hóa dữ liệu và đòi tiền chuộc, ảnh hưởng tới nhiều tổ chức, cá nhân trên phạm vi toàn cầu.

Nhằm phòng ngừa và ngăn chặn sự ảnh hưởng của mã độc máy tính WannaCry đến hệ thống thông tin các cơ quan nhà nước, người dân, doanh nghiệp và các tổ chức trên địa bàn tỉnh, Sở Thông tin và Truyền đề nghị các đơn vị thực hiện ngay một số giải pháp của Bộ Thông tin và Truyền thông, cụ thể 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 hoặc tìm kiếm theo từ khóa bản cập nhật KB4012598 trên trang chủ của Microsoft;

- Cập nhật ngay các chương trình diệt Virus (Antivirus) 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;

- Cẩn trọng khi nhận được thư điện tử (Email) có đính kèm các tập tin (File) hoặc các đường dẫn (Link) lạ được gửi trong Email, trên các mạng xã hội, công cụ chat…;

- 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;

- Thực hiện biện pháp sao lưu (Backup) dữ liệu quan trọng sang các thiết bị lưu trữ ngoài (USB, Ổ cứng xách tay…);

2 Đối với cơ quan, tổ chức, doanh nghiệp *(cụ thể với các quản trị viên hệ thống)*:

- 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 đặc thù riêng cho các máy chủ Windows của đơn vị. 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 tổ chức 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, để là xác định được các máy tính bị nhiễm trong mạng và có biện pháp xử lý kịp thời:

http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com/

…

<Domains này đã được sinkholed, danh sách sẽ được cập nhật liên tục trên Website>

- Cân nhắc Block việc sử dụng Tor trong mạng doanh nghiệp, tổ chức;

- Thực hiện biện pháp Backup dữ liệu quan trọng ngay;

- Cảnh báo đến người dùng trong đơn vị và thực hiện các biện pháp như đã nêu tại phần "Đối với cá nhân";

- Đăng tải nội dung này trên Cổng/Trang thông tin điện tử của đơn vị.

Trong quá trình triển khai, nếu có vướng mắc liên hệ Phòng Điều hành Cổng thông tin điện tử - Trung tâm Công nghệ thông tin và Truyền thông, điện thoại: 02973.680.682, di động: 0918.767.498 (Đ/c Thiện Nghi), email: ttnghi.stttt@kiengiang.gov.vn.

Nơi nhận:
- Như trên;
- Lưu VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG TỈNH KIÊN GIANG

Nguyễn Hồ Phương