

**ỦY BAN NHÂN DÂN
TỈNH THỪA THIÊN HUẾ**

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

Số: 3107/UBND-CNTT

Thừa Thiên Huế, ngày 16 tháng 5 năm 2017

V/v triển khai ngăn chặn, phòng ngừa
mã độc WannaCrypt lây lan, phát tán

Kính gửi:



- Các cơ quan chuyên môn trực thuộc UBND tỉnh;
- UBND các huyện, thị xã và thành phố Huế.

Hiện nay, mã độc tấn công đòi tiền chuộc (ransomware) có tên WannaCrypt (WanaCrypt0r) đang khai thác một số lỗ hổng trên các máy tính 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. UBND tỉnh yêu cầu các cơ quan, đơn vị tổ chức thực hiện các biện pháp phòng tránh và xử lý khẩn cấp mã độc này như sau:

1. Các biện pháp phòng tránh và xử lý khẩn cấp mã độc:

- Chỉ đạo cán bộ chuyên trách CNTT thực hiện cập nhật ngay các phiên bản hệ điều hành Windows đang sử dụng tại cơ quan, đơn vị. Cán bộ chuyên trách CNTT thực hiện các hướng dẫn phòng tránh và xử lý mã độc theo hướng dẫn gửi kèm;

- Cập nhật ngay các chương trình diệt virus đang sử dụng. Đối với các máy tính không có phần mềm diệt virus cần tiến hành cài đặt ngay phần mềm diệt virus có bản quyền;

- Cảnh trọng khi nhận được email có đính kèm và các liên kết (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 liên kết (link), nếu có nghi ngờ cần liên hệ với cán bộ chuyên trách CNTT ngay;

2. Do tính chất nguy hiểm của mã độc này, để đề phòng việc lây nhiễm và xảy ra sự cố mất dữ liệu nghiêm trọng, UBND tỉnh yêu cầu thủ trưởng các cơ quan, đơn vị gấp rút tổ chức triển khai các biện pháp phòng chống và cảnh báo nêu trên./.

Nơi nhận:

- Như trên;
- Tỉnh ủy, TT. HĐND (để báo cáo);
- UBND tỉnh: CT và các PCT UBND tỉnh;
- VP: CVP và các PCVP;
- Lưu: VT, DL, NC, CNTT.



Đặng Ngọc Trân



PHỤ LỤC

Ban hành kèm theo Công văn số 3107 /UBND-CNTT ngày 16 /5/2017

HƯỚNG DẪN phòng tránh và xử lý mã độc

1. Quét và dò tìm mã độc

- Thực hiện lệnh quét virusscan cho vùng Critical Areas, nếu phát hiện malware dạng MEM:Trojan.Win64.EquationDrug.gen cần khởi động lại máy tính ngay.
- Bật tính năng System Watcher để phân tích hành vi, phát hiện sớm mã độc nguy hiểm.
- Cài đặt các update hệ điều hành, đặc biệt là bản vá MS17-010 – Critical; kiểm tra thông tin về các phiên bản Windows bị ảnh hưởng và tải về bản vá lỗi EternalBlue (MS17-010) để cài đặt bản vá bảo mật Security Update for Microsoft Windows SMB Server (MS17-010 – Critical). Riêng đối với các máy tính sử dụng Windows XP, sử dụng bản vá: Security Update for Windows XP SP3 (KB4012598) hoặc tìm kiếm theo từ khóa bản cập nhật KB4012598 trên trang chủ của Microsoft;
- Có thể sử dụng công cụ quét và dò tìm mã độc của BKAV tại địa chỉ sau: <http://www.bkav.com.vn/Tool/CheckWanCry.exe>
- Cảnh báo tới người dùng trong đơn vị và thực hiện các biện pháp như nêu trên đối với người dùng.
- Trong trường hợp phát hiện máy tính bị lây nhiễm, không làm theo các hướng dẫn của hacker để tránh mất tiền và lây nhiễm virus thêm.
- Xác định và ngắt máy tính bị lây nhiễm khỏi hệ thống mạng, cập nhật chương trình diệt virus và quét lại toàn bộ máy tính để làm sạch virus trước khi cài đặt lại.
- Liên hệ ngay với Trung tâm EDIC hoặc Trung tâm Tin học Hành chính để được hỗ trợ khi cần thiết.

2. Thực hiện các thao tác trên và triển khai lưu trữ (backup) dữ liệu quan trọng ngay lập tức theo thứ tự ưu tiên các máy tính có chứa dữ liệu quan trọng. UBND các huyện, thị xã và thành phố Huế tổ chức hướng dẫn, triển khai các biện pháp phòng tránh và xử lý khẩn cấp mã độc đối với UBND các đơn vị cấp xã./.

ỦY BAN NHÂN DÂN TỈNH