

Số: 470/STTTT-CNTT

Thừa Thiên Huế, ngày 16 tháng 5 năm 2017

Về việc theo dõi ngăn chặn kết nối máy chủ
điều khiển mã độc WannaCry

Kính gửi:

- Các sở, ban, ngành cấp tỉnh;
- Các đơn vị sự nghiệp thuộc tỉnh;
- UBND các huyện, thị xã và thành phố Huế.



Sở Thông tin và Truyền thông nhận được Công văn số 144/VNCert-ĐPƯC ngày 13/5/2017 của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam – Bộ Thông tin và Truyền thông về việc theo dõi ngăn chặn kết nối máy chủ điều khiển mã độc WannaCry. Đây là mã độc nguy hiểm 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. Mã độc trên có tốc độ lan truyền với tốc độ nhanh chóng, nguy cơ ảnh hưởng đến hệ thống máy tính của tỉnh là rất lớn. Trước tình hình đó, Sở Thông tin và Truyền thông đề nghị các đơn vị triển khai một số biện pháp sau đây:

1. Kịp thời cung cấp thông tin cụ thể về diễn biến và các biện pháp phòng chống, khắc phục sự cố do mã độc tổng tiền gây ra đến các cơ quan báo chí, truyền thông, các đơn vị đang triển khai vận hành, ứng dụng các hệ thống thông tin của tỉnh.
2. Các cơ quan đơn vị thường xuyên cung cấp tình hình diễn biến và mức độ lan truyền, triển khai các biện pháp phòng ngừa và khắc phục sự cố.
3. Lãnh đạo các cơ quan đơn vị chủ động trong công tác phòng chống mã độc, thường xuyên kiểm tra giám sát hệ thống CNTT của đơn vị để kịp thời phát hiện các dấu hiệu bất thường và thông báo cho Sở Thông tin và Truyền thông để phối hợp các đơn vị kịp thời khắc phục sự cố.
4. 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.
5. Cập nhật ngay các chương trình 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 có bản quyền.
6. Cảnh trọng khi nhận được email có đính kèm và các đường liên kết lạ được gửi trong email, trên các mạng xã hội, công cụ chat.
7. 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.

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

9. Tuyệt đối không truy cập các tập tin như sau: @WanaDecryptor@.exe, b.wnry, c.wnry, s.wnry taskdl.exe, taskse.exe, t.wnry, u.wnry, các file với phần mở rộng “.wnry”, các file với phần mở rộng “.WNCRY”.

10. Thực hiện biện pháp lưu trữ (backup) dữ liệu quan trọng của đơn vị.

Đây là nhiệm vụ cấp bách cần thiết phải thực hiện ngay để phòng tránh mã độc nguy hiểm trên môi trường mạng, Sở Thông tin và Truyền thông tỉnh Thừa Thiên Huế kính gửi đến các đơn vị để các đơn vị triển khai thực hiện./.

Ghi chú:

- Các sở, ban ngành cấp tỉnh có nhiệm vụ thông báo cho các đơn vị sự nghiệp trực thuộc;

- UBND các huyện, thị xã, thành phố thông báo cho các phòng, ban, các xã, phường, thị trấn triển khai.

Nơi nhận:

- Như trên;
- UBND tỉnh (để b/c);
- BCĐ ATTT mạng (để b/c);
- Các PGĐ Sở;
- Lưu: CNTT, VT

A. 2/2018

GIÁM ĐỐC



Lê Sĩ Minh