UBND TỈNH QUẢNG BÌNH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 496 /STTTT-CNTT

V/v cảnh báo về biến thể mới của mã độc tống tiền Ransomware (mã độc Petya)

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

Quảng Bình, ngày 29 tháng 6 năm 2017

Kính gửi:

- Văn phòng Tỉnh ủy, Văn phòng HĐND tỉnh;
- Các Sở, ban, ngành, đoàn thể cấp tỉnh;
- Các huyện, thành, thị ủy;
- UBND các huyện , thị xã, thành phố;
- Các cơ quan Trung ương trên địa bàn tỉnh.

Ngày 28/6/2017, Cục an toàn thông tin - Bộ Thông tin và Truyền thông có Công văn số 338/CATTT-TĐQLGS về việc cảnh báo về biến thể mới của mã độc tống tiền Ransomware (mã độc Petya). Theo đó, mã độc Petya khi lây nhiễm vào máy tính sẽ không mã hóa từng tập tin, mà thực hiện mã hóa Bảng File (Master File Table – MFT, chứa thông tin về tất cả các tập tin và thư mục trong phân vùng) và thay thế Master Boot Record của máy tính bằng tập tin độc hại để hiển thị thông tin đòi tiền chuộc. Do vậy máy tính người dùng sẽ không thể khởi động được khi bị nhiễm mã độc này *(Sở Thông tin và Truyền thông đã chuyển Công văn này đến toàn thể các thành viên Tổ Ứng cứu sự cố của tỉnh)*.

Một số hòm thư điện tử dùng để phát tán mã độc Petya:

- wowsmith123456@posteo.net
- iva76y3pr@outlook.com
- carmellar4hegp@outlook.com
- amanda44i8sq@outlook.com

Để kịp thời cảnh báo, phát hiện và ngăn chặn nguy cơ mất an toàn thông tin từ loại mã độc này, Sở Thông tin và Truyền thông đề nghị quý cơ quan, đơn vị chỉ đạo cán bộ phụ trách công nghệ thông tin thực hiện các nội dung sau:

- Kiểm tra và bảo đảm các máy tính trong hệ thống mạng đã vá các bản vá bảo mật, đặc biệt là MS17-010, CVE 2017-0199;

- Chặn toàn bộ kết nối liên quan đến dịch vụ SMB (445/137/138/139) từ ngoài Internet;

- Vô hiệu hóa WMIC (Windows Management Instrumentation Command-line);

- Không truy cập vào các liên kết lạ, cảnh giác cao khi mở các tập tin đính kèm trong thư điện tử;

- Sao lưu các dữ liệu quan trọng thường xuyên vào các thiết bị lưu trữ riêng biệt;

- Cập nhật phần mềm diệt virus;

- Tắt dịch vụ SMB trên tất cả các máy trong mạng LAN (nếu không cần thiết);

- Tạo tệp tin " C:\Windows\perfc " để ngăn ngừa nhiễm ransomware. Đây là tập tin mã độc kiểm tra trước thực hiện các hành vi độc hại trên máy tính.

- Thường xuyên cập nhật vào chuyên mục An toàn thông tin trên Trang thông tin điện tử của Sở Thông tin và Truyền thông để kịp thời nắm bắt thông tin về mã độc và các hướng dẫn xử lý.

Quá trình thực hiện nếu có vướng mắc xin liên hệ về phòng Công nghệ thông tin, Sở Thông tin và Truyền thông (điện thoại 0232.3851206) để phối hợp thực hiện.

Trân trọng./.

Nơi nhận:
- Như trên;
- Cục An toàn thông tin {báo cáo};
- Trung tâm CNTT&TT {để phối hợp};
- Lưu: CNTT, VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH NINH BÌNH

Nguyễn Phi Khanh