UBND TỈNH QUẢNG BÌNH
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG

Số: 1222/STNMT- 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 04 tháng 7 năm 2017

TT CÔNG NGHỆ THÔNG TIN TN&MT QB
ĐẾN Số: 734
Ngày: 04/7/2017

Kính gửi: Các phòng, đơn vị trực thuộc.

Sở Tài nguyên và Môi trường nhận được cảnh báo khẩn cấp của Cục an toàn thông tin - Bộ Thông tin và Truyền thông về việc cảnh báo về biến thể mới của mã độc tống tiền Ransomware (mã độc Petya). Mã độc Petya có hoạt động rất khác so với các biến thể Ransomware khác. 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, máy tính người dùng sẽ không thể khởi động được khi bị nhiễm mã độc.

Xác định mức độ nguy hiểm và nguy cơ lây nhiễm cao, Sở Tài nguyên và Môi trường yêu cầu các phòng, đơn vị trực thuộc thực hiện các nội dung sau:

1. Thông báo đến tất cả các cán bộ, công chức, viên chức và người lao động kiểm tra máy tính đang sử dụng và làm theo các bước hướng dẫn để ngăn chặn kết nối máy chủ có chứa mã độc Petya *(có hướng dẫn kèm theo)*.

2. Trung tâm Công nghệ thông tin Tài nguyên và Môi trường thực hiện các biện pháp đảm bảo an toàn thông tin theo cảnh báo số 338/CATTT-TĐQLGS của Cục an toàn thông tin – Bộ Thông tin và Truyền thông.

3. Khi có sự cố đề nghị liên hệ Trung tâm Công nghệ thông tin Tài nguyên và Môi trường, điện thoại : 0232.3825742 để ứng cứu và xử lý kịp thời.

Yêu cầu các phòng, đơn vị trực thuộc nghiêm túc triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Lãnh đạo Sở;
- Lưu VT, TTCNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG
TỈNH QUẢNG BÌNH

Phạm Văn Lương

HƯỚNG DẪN KIỂM TRA, NGĂN CHẶN MÃ ĐỘC PETYA.

(Kèm theo công văn số 1222/STNMT-CNTT ngày 04 tháng 7 năm 2017)

I. Hiện tượng khi máy tính lây nhiễm mã độc

+ Khi lây nhiễm máy tính tự động kết nối mạng đến một số địa chỉ: 185.165.29.78; 84.200.16.242; 111.90.139.247; 95.141.115.108 (Nguồn:https://gist.githubusercontent.com/vulnersCom/65fe44d27d29d7a5de4c176baba45759/raw/b414f3162198d7fa117bb934a92124d7075b3f5e/Petya_ransomware.txt).

II. Biện pháp bảo đảm an toàn thông tin

+ Không click vào 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

+ Kiểm tra và bảo đảm các máy tính trong hệ thống mạng đã vá các bản vá bảo mật, đặc biệt là MS 17-010, CVE 2017-0199; 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, MS 17-010, CVE 2017-0199 trên trang chủ của Microsoft

+ 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;

+ Tạo tệp tin Folder " C:\Windows\perfc " để ngăn ngừa nhiễm ransomware.

III. Trung tâm Công nghệ thông tin Tài nguyên và Môi trường thực hiện các biện pháp trên máy chủ

+ Vô hiệu hóa công cụ WMIC (Windows Management Instrumentation Command-line), công cụ có sẵn trong Windows cho phép truy cập và thiết lập cấu hình trên các máy tính Windows ;

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

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