UBND TỈNH QUẢNG BÌNH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 662/STTTT-CNTT

Quảng Bình, ngày 04 tháng 8 năm 2016

V/v theo dõi, ngăn chặn kết nối và Xoá các tệp tin chứa mã độc

Kính gửi:
- Các sở, ban, ngành cấp tỉnh;
- UBND các huyện, thị xã, thành phố;
- Các tổ chức Chính trị, xã hội trên địa bàn tỉnh.

Thực hiện Quyết định số 26/2014/QĐ-UBND ngày 21/10/2014 của UBND tỉnh Quảng Bình về việc ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Quảng Bình, Công văn số 238/VNCERT-ĐPƯC ngày 03/8/2016 của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam về việc theo dõi, ngăn chặn kết nối và xoá các tệp tin chứa mã độc; Sở Thông tin và Truyền thông đề nghị Lãnh đạo các sở, ban, ngành, địa phương chỉ đạo các đơn vị thuộc phạm vi quản lý thực hiện khẩn cấp các công việc sau:

1. Theo dõi và ngăn chặn kết nối đến các tên miền sau:

a) playball.ddns.info

b) nvedia.ddns.info

c) air.dcsvn.org

2. Rà quét hệ thống, xóa các thư mục và tập tin mã độc có kích thước tương ứng:

a) C://Program Files\Common Files\ McAfee\McAfee.exe (137.28 KB)

- MD5: 884D46C01C762AD6DDD2759FD921BF71

- SHA-1: D201B130232E0EA411DAA23C1BA2892FE6468712

b) C:\Program Files\Common Files\McAfee\McUtil.dll (3.50 KB)

- MD5: C52464E9DF8B3D08FC612A0F11FE53B2

- SHA-1: E4646D10AD93600232D7A24856D69F00510949A40

c) C:\Windows\system32\DiskMgers.dll (85.00 KB)

- MD5: 9BF793EF195CC62F8A61093F77B03158

- SHA-1: 46844B0ACF2BB67ADBF2304A61BE07738D2DDD64

d) Tập tin "diskperf.exe": tìm tất cả các file trong ổ Hệ điều hành có:

- MD5: 29E65E1256FC998B7CE8494656B3EF8

- SHA-1: 8C073B63D85CBF48BD742A62C7A59EEB064DA74D

3. Hướng dẫn kiểm tra kiểm tra mã MD5, SHA-1 của tập tin và cách thức xóa tập tin chứa mã độc trong phụ lục kèm theo.

Trên đây là những mã độc đặc biệt nguy hiểm, nếu bị lây nhiễm, hệ thống có thể bị đánh cắp thông tin và bị phá huỷ. Đề nghị các Lãnh đạo các cơ quan, đơn vị khẩn trương, nghiêm túc thực hiện các hướng dẫn. Sau khi thực hiện kiểm tra, rà soát, các đơn vị tổng hợp, báo cáo về Sở Thông tin và Truyền thông Quảng Bình trước 16h00 ngày 10/8/2016; bản điện tử gửi về địa chỉ email: ttdldt@quangbinh.gov.vn. Mọi yêu cầu hỗ trợ xin liên lạc về phòng CNTT (đồng chí Nguyễn Vĩnh Huế) theo số điện thoại: 0523.856696.

Rất mong sự hợp tác của các cơ quan, đơn vị./.

Nơi nhận:
- Như trên;
- Giám đốc sở {báo cáo};
- TTCNTT-TT {thực hiện}
- Lưu VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Nguyễn Phi Khanh

PHỤ LỤC

Hướng dẫn kiểm tra mã MD5, SHA-1 của tập tin và cách thức xóa tập tin chứa mã độc

(Kèm theo Công văn số /STTTT-CNTT ngày 04/8/2016)

1. Hướng dẫn kiểm tra mã hash MD5, SHA-1:

a) Download phần mềm tại http://www.nirsoft.net/utils/hashmyfiles.zip;

b) kiểm tra: giải nén tập tin hashmyfiles.zip ở trên, tiếp hành mở file "HashMyFiles.exe". Nhấn vào File -> Add Files. Tiếp đó, trỏ đến file cần kiểm tra mã Hash. Mã MD5 và SHA-1 sẽ hiển thị bên khung chương trình. Đơn vị chỉ cần đối chiếu mã MD5 và SHA-1 tương ứng ở trên.

2. Hướng dẫn gỡ bỏ tập tin chứa mã độc:

a) Xác định mã độc là: nếu mã MD5 và SHA-1 trùng nhau thì tập tin trên máy tính là phần mềm có chứa mã độc; nếu không trùng thì chưa khẳng định 100% nos không phải là mã độc và có thể không xóa trong trường hợp này.

b) Cách thức xóa tập tin chứa mã độc được thực hiện như sau: do tập tin này đang chạy nên ta cần dừng hoặc tắt tiến trình này trước khi xóa. Trước tiên cần tải phần mềm miễn phí có tên "Process Explorer" của Microsoft tại địa chỉ: https://download.sysinternals.com/files/ ProcessExplorer.zip.

Sau khi tải về giải nén ta chạy file "procexp.exe", tiế hành tìm kiếm các tiến trình tương ứng trong văn bản trên và nhấn chuột phải chọn "Suspend" hoặc "Kill Process". Sau khi chọn xong, ta vào đường dẫn tương ứng để xóa.