

PHIẾU GIẢI QUYẾT VĂN BẢN ĐẾN

**SỞ Y TẾ
TỈNH KHÁNH HÒA**

Số đến:

Ngày đến:

Lưu hồ sơ:

Nơi ban hành:

Số và ký hiệu văn bản:

Ngày ban hành: Thời hạn xử lý:

Đơn vị chủ trì: Đơn vị phối hợp:

*Ý kiến của lãnh đạo cơ quan:

Chuyển VP & TP Mưu
trị Nhà TP. triu

Ngày 08 tháng 8 năm 2016

(Signature)

*Ý kiến của Trưởng/Phó đơn vị:

.....

.....

.....

*Ý kiến đề xuất của người giải quyết:

.....

.....

.....

*Tiên độ giải quyết:

Ngày chuyển VB:

Ngày trình VB trả lời:

Ngày ban hành VB trả lời:

Số, ký hiệu VB trả lời:

Đánh giá thời gian hoàn thành: Trước hạn

Đúng hạn

Trễ hạn

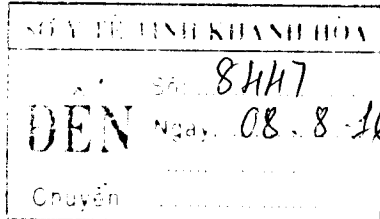


UBND TỈNH KHÁNH HÒA
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
Số: 1045/STTTT-CNTT

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc
Khánh Hòa, ngày 05 tháng 8 năm 2016

V/v đề nghị kiểm tra, theo dõi ngăn chặn kết nối
và xóa các tập tin chứa mã độc

Kính gửi:



- Văn phòng Tỉnh ủy;
- Các sở, ban, ngành;
- Ủy ban-nhân dân các huyện, thị xã, thành phố;
- Các đơn vị sự nghiệp thuộc Ủy ban nhân dân tỉnh;
- Các cơ quan ngành dọc Trung ương.

Sở Thông tin và Truyền thông nhận được Công văn số 238/VNCERT-ĐPUC ngày 03/8/2016 của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) về việc theo dõi, ngăn chặn kết nối và xóa các tập tin chứa mã độc.

Sở Thông tin và Truyền thông đề nghị Lãnh đạo các cơ quan, đơn vị tổ chức triển khai và chỉ đạo các đơn vị thuộc phạm vi quản lý thực hiện khẩn cấp các nội dung sau:

1. Kiểm tra, theo dõi và ngăn chặn kết nối từ hệ thống thông tin của cơ quan đến các tên miền sau:

- a) playball.ddns.info
- b) nvidia.ddns.info
- c) air.dcsvn.org

2. Rà quét hệ thống và xóa các thư mục và tập tin mã độc có tên và 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: E464D10AD93600232D7A24856D69F00510949A40
- 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: 29E656E1256FC998B7CE8494656B3EF8
 - SHA-1: 8C073B63D85CBF48BD742A62C7A59EEB064DA74D

Những mã độc trên đặc biệt nguy hiểm, có thể đánh cắp thông tin và phá hủy hệ thống, Sở Thông tin và Truyền thông đề nghị Quý cơ quan, đơn vị nghiêm túc thực hiện theo Hướng dẫn kiểm tra mã MD5, SHA-1 của tập tin và cách thức xóa tập tin chức mã độc theo Phụ lục đính kèm Công văn này.

Sau khi thực hiện, đề nghị Quý cơ quan, đơn vị báo cáo tình hình và kết quả thực hiện về Sở Thông tin và Truyền thông qua phần mềm Quản lý văn bản và Điều hành (E-office) hoặc địa chỉ thư điện tử: cntt.stttt@khanhhoa.gov.vn trước ngày 15/8/2016 để tổng hợp, báo cáo Ủy ban nhân dân tỉnh.


Quá trình thực hiện nếu có vướng mắc hoặc cần hỗ trợ, đề nghị Quý cơ quan, đơn vị liên hệ: Phòng Công nghệ thông tin - Sở Thông tin và Truyền thông, điện thoại: 0583.563533 (gặp chị Nga - DD: 0947044099).

Trân trọng./.

Nơi nhận:

- Như trên (VB điện tử);
- UBND tỉnh (VB điện tử, để b/cáo);
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC



Nguyễn Thị Trung Thu



PHỤ LỤC

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

Kèm theo Công văn số: 1045/STTTT-CNTT ngày 05/8/2016 của Sở Thông tin và Truyền thông

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

a) Download phần mềm: <http://www.nirsoft.net/utils/hashmyfiles.zip>

b) Kiểm tra: Giải nén tập tin hashmyfiles.zip trên, tiến hành mở file "HashMyFiles.exe". Nhấn vào File -> Add Files; Trở đến file cần kiểm tra mã Hash. Mã MD5 và SHA-1 sẽ hiển thị bên khung chương trình. Bạn chỉ cần đối chiếu mã MD5 và SHA-1 tương ứng trong Công văn đi kèm.

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

a) Xác định mã độc: 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% nó không phải là mã độc. Có thể không xóa trong trường hợp này.

b) Cách xóa tập tin chứa mã độc: 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 bên dưới:
<https://download.sysinternals.com/files/ProcessExplorer.zip>

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

DANH SÁCH GỬI CÔNG VĂN.

STT	Tên cơ quan, đơn vị
1.	Văn phòng Tỉnh ủy
2.	Văn phòng Đoàn ĐBQH&HĐND tỉnh
3.	Văn phòng UBND tỉnh Khánh Hòa
4.	Sở Công thương
5.	Sở Tài chính
6.	Sở LĐTĐ và XH
7.	Sở Y tế
8.	Sở Tư pháp
9.	Sở Tài nguyên và Môi trường
10.	Sở Kế hoạch và Đầu tư
11.	Sở Giao thông - Vận tải
12.	Sở Nông nghiệp và Phát triển Nông thôn
13.	Sở Văn hóa, Thể thao, Du lịch
14.	Sở Khoa học và Công nghệ
15.	Sở Xây dựng
16.	Sở Giáo dục và Đào tạo
17.	Sở Nội vụ
18.	Sở Ngoại vụ
19.	Sở Du lịch
20.	Ban Dân tộc
21.	Ban QL khu KT Vân Phong
22.	Công an tỉnh
23.	Bộ Chỉ huy quân sự tỉnh
	UBND các huyện, thị xã, thành phố
24.	UBND thành phố Nha Trang
25.	UBND thành phố Cam Ranh
26.	UBND thị xã Ninh Hòa
27.	UBND huyện Vạn Ninh
28.	UBND huyện Diên Khánh
29.	UBND huyện Khánh Vĩnh
30.	UBND huyện Khánh Sơn
31.	UBND huyện Cam Lâm
	Các cơ quan ngành dọc TW
32.	Cục Thuế tỉnh
33.	Cục Hải quan tỉnh
34.	Cục Thống kê
35.	Bảo hiểm xã hội tỉnh
36.	Ngân hàng nhà nước tỉnh
37.	Tòa án nhân dân tỉnh
38.	Viện Kiểm sát nhân dân tỉnh