1204/STTTT-CNTT
Sở Thông tin và Truyền thông
sttt@danang.gov.vn
06.06.2018 11:21:11 +07:00

UBND THÀNH PHỐ ĐÀ NẴNG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1204 /STTTT-CNTT

V/v cảnh báo mã độc mới VPNfilter

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

Đà Nẵng, ngày 06 tháng 6 năm 2018

Kính gửi:
- Các sở, ban, ngành;
- UBND các quận huyện, phường xã;
- Các cơ quan Đảng, Mặt trận, tổ chức chính trị - xã hội;
- Các cơ quan Trung ương trên địa bàn thành phố;
- Các doanh nghiệp CNTT trên địa bàn thành phố.

Thực hiện chức năng theo dõi, giám sát an toàn thông tin mạng trên địa bàn thành phố Đà Nẵng, Sở Thông tin và Truyền thông cảnh báo mã độc mới VPNfilter như sau:

1. Mã độc VPNFilter là mối đe dọa mới đối với các thiết bị định tuyến router và thiết bị lưu trữ NAS trên quy mô toàn cầu. Không giống như hầu hết các mối đe dọa đối với các thiết bị IoT khác, VPNFilter có khả năng duy trì sự hiện diện liên tục trên thiết bị bị lây nhiễm, ngay cả sau khi khởi động lại. VPNFilter có khả năng làm gián điệp lưu lượng truy cập được định tuyến thông qua thiết bị, làm tê liệt các thiết bị và ngăn chặn kết nối trên môi trường mạng.

Khi đã lây nhiễm thành công, VPNFilter sẽ khởi động lại thiết bị. Từ đó, nó tạo được kết nối lâu dài và cài đặt mã độc phục vụ cho giai đoạn hai. Đặc trưng của mạng botnet sử dụng mã độc VPNFilter là thư mục có đường dẫn /var/run/vpnfilterw được tạo ra trong quá trình cài đặt.

Theo thông tin từ các chuyên gia trên thế giới, mã độc này đã ảnh hưởng đến 500.000 thiết bị định tuyến của khách hàng tại 54 quốc gia trên thế giới, bao gồm Việt Nam. Các thiết bị đã bị phát hiện bị ảnh hưởng của mã độ bao gồm các thiết bị định tuyến Linksys, MikroTik, Netgear and TP-Link và thiết bị lưu trữ của QNAP.

2. Để đảm bảo an toàn, an ninh thông tin đối với các hệ thống thông tin trên địa bàn thành phố, Sở Thông tin và Truyền thông kính đề nghị các cơ quan, đơn vị:

a) Kiểm tra, rà soát các thiết bị hiện có của đơn vị nằm trong danh mục thiết bị có khả năng lây nhiễm cao tại Phụ lục kèm theo Công văn này; cài đặt lại thiết bị về mặc định để xóa mã độc và cập nhật chương trình cơ sở (firmware) của các thiết bị;

`

b) Cài đặt mật khẩu truy cập các thiết bị với độ khó cao và đặc biệt lưu ý không sử dụng mật khẩu mặc định để truy cập vào thiết bị.

Sở Thông tin và Truyền thông kính đề nghị Quý cơ quan, đơn vị triển khai thực hiện. Thông tin chi tiết vui lòng liên hệ ông Phạm Thanh Sơn, Chuyên viên Phòng Công nghệ thông tin, Sở Thông tin và Truyền thông (Điện thoại IP 6207, điện thoại cố định 0236 3840125, di động 01684157558, email sonpt2@danang.gov.vn)./.

Nơi nhận:
- Như trên;
- Giám đốc Sở (báo cáo);
- Trung tâm IID, Trung tâm DNICT;
- Tạp chí ICT, Trang TTĐT Sở;
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Trần Ngọc Thạch

Phó Giám đốc
Trần Ngọc Thạch
06.06.2018
07:58:47
+07:00

Phụ lục

DANH MỤC THIẾT BỊ CÓ KHẢ NĂNG LÂY NHIỄM CAO

(*Kèm theo Công văn số /STTTT-CNTT ngày tháng 6 năm 2018 của Sở Thông tin và Truyền thông*)

STT	Tên thiết bị
1	Linksys E1200
2	Linksys E2500
3	Linksys WRVS4400N
4	Mikrotik RouterOS for Cloud Core Routers: Versions 1016, 1036, and 1072
5	Netgear DGN2200
6	Netgear R6400
7	Netgear R7000
8	Netgear R8000
9	Netgear WNR1000
10	Netgear WNR2000
11	QNAP TS251
12	QNAP TS439 Pro
13	Other QNAP NAS devices running QTS software
14	TP-Link R600VPN