UBND TỈNH KHÁNH HÒA
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 485/STTTT-CNTT

Khánh Hòa, ngày 20 tháng 3 năm 2019

V/v cảnh báo theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc GrandCrab 5.2

Kính gửi:
- Các Sở, ban, ngành;
- Ủy ban nhân dân các huyện, thị xã, thành phố;
- Các đơn vị sự nghiệp trực thuộc Ủy ban nhân dân tỉnh;
- Các cơ quan ngành dọc Trung ương.

Sở Thông tin và Truyền thông nhận được Công văn số 81/VNCERT-ĐPƯC ngày 15/3/2019 của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) – Bộ Thông tin và Truyền thông về việc theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc GrandCrab 5.2.

Theo nội dung cảnh báo của Trung tâm VNCERT tại Công văn nêu trên, GrandCrab 5.2 là phiên bản mới trong họ mã độc tống tiền GrandCrab đã lan rộng trên toàn cầu trong hơn một năm qua. Ngày 05/4/2018, Trung tâm VNCERT đã phát hành Công văn số 58/VNCERT-ĐPƯC về việc ngăn chặn kết nối máy chủ điều khiển mã độc GrandCrab (phiên bản 1.0 và 2.0) *và hiện nay Trung tâm VNCERT cũng đã hỗ trợ giải pháp giải mã GranCrab phiên bản 5.1 trở về trước.*

Tuy nhiên, qua theo dõi không gian mạng, Trung tâm VNCERT phát hiện giữa tháng 3/2019 đến nay đang có chiến dịch phát tán mã độc tống tiền GrandCrab 5.2 vào Việt Nam và các nước Đông Nam Á. Tại Việt Nam, GrandCrab 5.2 được phát tán thông qua thư điện tử giả mạo từ Bộ Công an Việt Nam với tiêu đề *"Goi trong Cong an Nhan dan Viet Nam"*, có đính kèm tệp documents.rar. Khi người dùng giải nén và mở tệp tin đính kèm, mã độc sẽ được kích hoạt và toàn bộ dữ liệu người dùng bị mã hóa, đồng thời sinh ra một tệp nhằm yêu cầu và hướng dẫn người dùng trả tiền chuộc từ 400 – 1.000 USD bằng cách thanh toán qua đồng tiền điện tử để giải mã dữ liệu.

Để kịp thời triển khai các biện pháp ngăn chặn nguy cơ lây nhiễm và phát tán mã độc nguy hiểm nêu trên, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị, địa phương thực hiện khẩn cấp các việc sau để phòng ngừa, ngăn chặn việc tấn công của mã độc GranCrab 5.2, cụ thể như sau:

1. Theo dõi, ngăn chặn kết nối đến các máy chủ điều khiển mã độc tống tiền GrandCrab và cập nhật vào hệ thống bảo vệ như : IDS/IPS, Firewall,... theo các thông tin nhận dạng *tại Phụ lục đính kèm Công văn này*;

2. Nếu phát hiện các dấu hiệu bị nhiễm mã độc, cần nhanh chóng cô lập vùng/máy đã phát hiện;

3. Thông báo người sử dụng nâng cao cảnh giác, không mở và click vào các liên kết cũng như các tập tin đính kèm trong thư điện tử có chứa các tập tin dạng .doc,.pdf,.zip,.rar... được gửi từ người lạ hoặc nếu thư điện tử được gửi từ người quen nhưng cách đặt tiêu đề hoặc ngôn ngữ khác thường; đồng thời, thông báo cho bộ phận chuyên trách quản trị hệ thống hoặc đảm bảo an toàn thông tin khi gặp tập tin nghi ngờ.

4. Khẩn trương thông báo nội dung văn bản này đến tất cả các cơ quan, đơn vị trực thuộc để tổ chức triển khai thực hiện.

Sau khi triển khai các biện pháp nêu trên, đề nghị Quý cơ quan báo cáo kết quả thực hiện và tổng hợp tình hình thông tin mã độc phát hiện, xử lý được (nếu có) về Sở Thông tin và Truyền thông qua phần mềm E-Office hoặc địa chỉ thư điện tử cntt.stttt@khanhhoa.gov.vn **trước ngày 29/3/2019** để tổng hợp, báo cáo Ủy ban nhân dân tỉnh và Trung tâm VNCERT.

Quá trình thực hiện nếu có vướng mắc hoặc cần hỗ trợ, đề nghị Quý cơ quan liên hệ đầu mối Thường trực Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa để phối hợp xử lý:

- Phòng Công nghệ thông tin – Sở Thông tin và Truyền thông;
- Địa chỉ: Nhà A1 Khu liên cơ số 01 Trần Phú, thành phố Nha Trang;
- Điện thoại: 0258.3563533;
- Thư điện tử: cntt.stttt@khanhhoa.gov.vn

Sở Thông tin và Truyền thông đề nghị Quý cơ quan quan tâm thực hiện.

Trân trọng./.

Nơi nhận:
- Như trên (VBĐT);
- UBND tỉnh (VBĐT, để b/c);
- Trung tâm VNCERT (VBĐT, để b/c);
- Lưu: VT, CNTT.

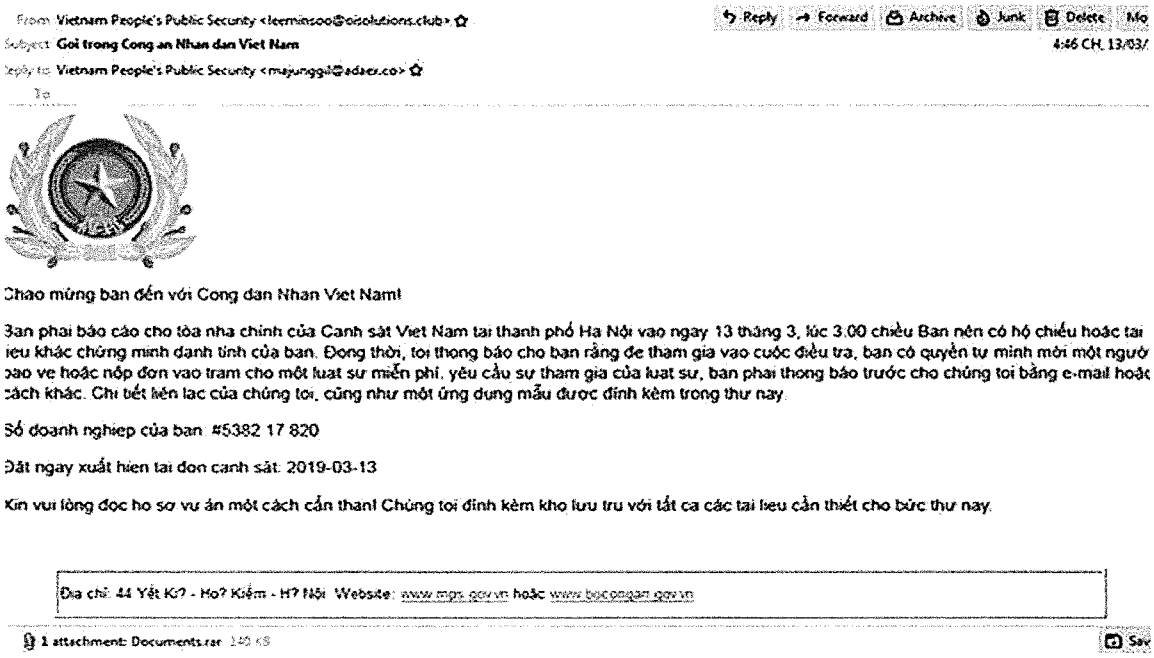
KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Ký bởi: Nguyễn Thị Trung Thu
Email: nttthu@khanhhoa.gov.vn
Cơ quan: Sở Thông tin và Truyền thông, Tỉnh Khánh Hòa
Thời gian ký: 20.03.2019 10:08:20 +07:00

Nguyễn Thị Trung Thu

PHỤ LỤC
THÔNG TIN VÀ MÃ ĐỘC GRANDCRAB PHIÊN BẢN 5.2
(Kèm theo Công văn số 485/STTTT-CNTT ngày 20/3/2018 của Sở Thông tin và Truyền thông)

1. Hình thức phát tán mã độc



2. Danh sách các máy chủ điều khiển mã độc (C&C Server)

TT	Địa chỉ C&C	Ghi chú
1	www.kakaocorp.link(IP :107.173.49.2008)	Phiên bản 5.2

3. Danh sách mã băm

	Hash	Ghi chú
MD5	DDCA6B2B2623904A072A5AF0A9E26267	Phiên bản 5.2
SHA1	E081D35048E2DE07BE34C0EAD3B9FD16F6BADB74	Phiên bản 5.2