UBND TỈNH SÓC TRĂNG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số:..172../STTTT-CNTT
V/v phòng ngừa, ngăn chặn mã độc GandCrap 5.2

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

Sóc Trăng, ngày 18 tháng 3 năm 2019

Kính gửi:
- Thủ trưởng các Sở, ban ngành tỉnh;
- Thủ trưởng các đơn vị sự nghiệp thuộc UBND tỉnh;
- Chủ tịch UBND các huyện, thị xã, thành phố, tỉnh Sóc Trăng.

Thực hiện Công văn số 81/VNCERT-ĐPƯC ngày 15/3/2019 của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) về việc theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc GandCrad 5.2,

Thông qua theo dõi của Trung tâm VNCERT từ giữa tháng 3/2019 đến nay đang có chiến dịch phát tán Mã độc tống tiền GandCrap 5.2 vào Việt Nam thông qua thư điện tử dưới hình thức giả mạo từ Bộ Công an Việt Nam với tiêu đề *"Goi trong Cong an Nhan dan Viet Nam"*, có đính kèm tập tin documents.rar. Khi người dùng giải nén và mở tệp 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) để giải mã dữ liệu.

Để kịp thời phòng ngừa, ngăn chặn nguy cơ mất an toàn thông tin, Sở Thông tin và Truyền thông đề nghị Lãnh đạo Quý cơ quan, đơn vị quan tâm chỉ đạo các đơn vị thuộc phạm vi quản lý thực hiện khẩn cấp các việc sau theo hướng dẫn của Trung tâm VNCERT để phòng ngừa, ngăn chặn việc tấn công của mã độc GandCrap 5.2, cụ thể như sau:

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

2. Nếu phát hiện mã độc GandCrab cần nhanh chóng cô lập vùng/máy bị nhiễm;

3. Khuyến cáo cán bộ, nhân viên nâng cao cảnh giác, không mở và click vào các liên kết (link) cũng như các tệp tin đính kèm trong email có chứa các tệp dịnh dạng .doc, .pdf, .zip… được gửi từ người lạ hoặc email được gửi từ người quen, nhưng cách đặt tiêu đề, ngôn ngữ khác thường và thông báo cho cán bộ chuyên trách công nghệ thông tin khi nhận được email nghi ngờ.

Mã độc tống tiền GandCrap rất nguy hiểm có thể đánh cắp thông tin và mã hóa toàn bộ dữ liệu trên máy bị nhiễm. Tin tặc có thể khai thác và tấn công gây nhiều hậu quả nghiêm trọng khác, Sở Thông tin và Truyền thông yêu cầu Lãnh đạo quý cơ quan, đơn vị quan tâm thực hiện.

Trong quá trình thực hiện, nếu có vướng mắc về kỹ thuật cần được hỗ trợ, xin liên hệ Phòng Nghiệp vụ Tổng hợp, Trung tâm Công nghệ thông tin và Truyền thông, điện thoại: 0299.3626600, Email: ict@soctrang.gov.vn./.

Nơi nhận:
- Như trên;
- TT-CNTT-TT (để hỗ trợ);
- Lưu VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

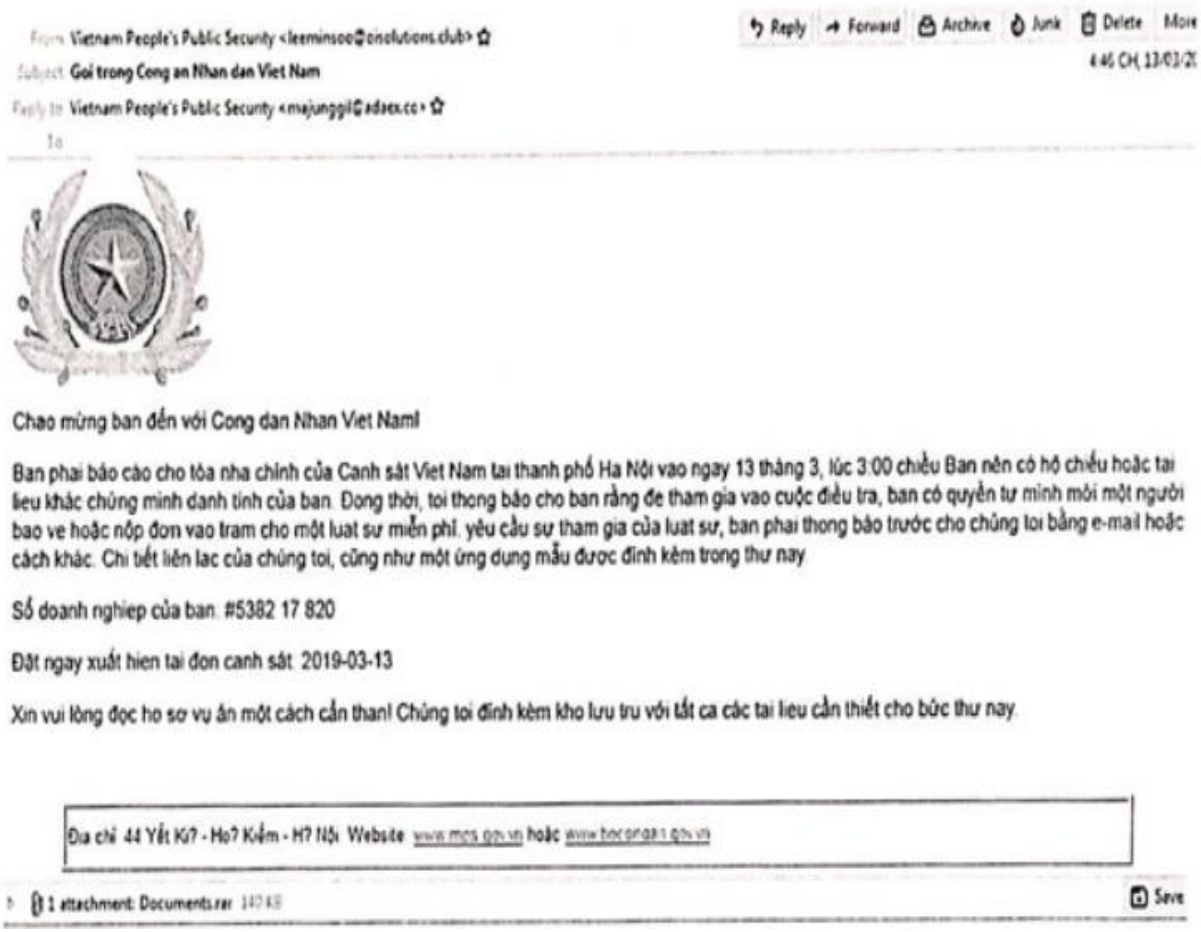
CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH SÓC TRĂNG

Ký bởi: Dương Văn Nhân
Email: dvnhan@soctrang.gov.vn
Cơ quan: Sở Thông tin và Truyền thông, Tỉnh Sóc Trăng
Ngày ký: 18.03.2019 10:27:49 +07:00

PHỤ LỤC
THÔNG TIN VỀ MÃ ĐỘC GANDCRAP 5.2

(Kèm theo Công văn số..172../STTTT-CNTT ngày 18/3/2019 của Sở Thông tin và Truyền thông tỉnh Sóc Trăng)

1. Hình thức phát tán mã độc



Hình ảnh tệp tin chứa mã độc đính kèm
Thư điện tử giả mạo từ Bộ Công an Việt Nam

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: 107.173.49.208)	Phiên bản 5.2

3. Danh sách mã băm

	Địa chỉ C&C	Ghi chú
MD5	DDCA6B2B2623904A072A5AF0A9E26267	Phiên bản 5.2
SHA1	E081D35048E2DE07BE34C0EAD3B9FD16F6BADB74	Phiên bản 5.2