BỘ KHOA HỌC VÀ CÔNG NGHỆ
TRUNG TÂM CÔNG NGHỆ THÔNG TIN

Số: 60 /TTCNTT-KTHT
V/v theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc GandCrab 5.2

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

Hà Nội, ngày 18 tháng 03 năm 2019

Kính gửi: Các đơn vị trực thuộc Bộ

Theo thông báo của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam tại công văn số 81/VNCERT-ĐPƯC ngày 15/3/2019, hiện nay đang có chiến dịch phát tán Mã độc tống tiền GandCrab 5.2 (là phiên bản mới trong họ Mã độc tống tiền GandCrab lan rộng trên toàn cầu trong hơn một năm qua) vào Việt Nam và các nước Đông Nam Á. Tại Việt Nam GandCrab 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 tin **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.

Thực hiện chức năng nhiệm vụ được giao về việc điều phối, ứng cứu sự cố an toàn thông tin mạng của Bộ KH&CN, Trung tâm Công nghệ thông tin yêu cầu các đơn vị trực thuộc Bộ thực hiện khẩn cấp việc phòng ngừa, ngăn chặn tấn công của mã độc GandCrab 5.2 như sau:

1. Theo dõi, ngăn chặn kết nối đến các máy chủ điều khiển mã độc tống tiền GandCrab 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 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. Và cần thông báo cho bộ phận chuyên trách quản trị hệ thống hoặc đảm bảo an toàn thông tin khi gặp nghi ngờ.

Mã độc tống tiền GandCrab rất nguy hiểm, có thể đánh cắp thông tin và mã hóa toàn bộ dữ liệu trên máy bị nhiễm. Tin tặc khai thác và tấn công sẽ gây ra nhiều hậu quả nghiêm trọng khác, Trung tâm Công nghệ thông tin yêu cầu Lãnh đạo các đơn vị nghiêm túc chỉ đạo thực hiện việc phòng ngừa, ngăn chặn sự tấn công của mã độc này.

Mọi chi tiết xin liên hệ Phòng Kỹ thuật hạ tầng – Trung tâm Công nghệ thông

tin theo số điện thoại: 024.39439060/ địa chỉ thư điện tử tiếp nhận báo cáo sự cố: phongktht@most.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Bùi Thế Duy (để b/c);
- Lưu: TTCNTT.

GIÁM ĐỐC

TRUNG TÂM CÔNG NGHỆ THÔNG TIN

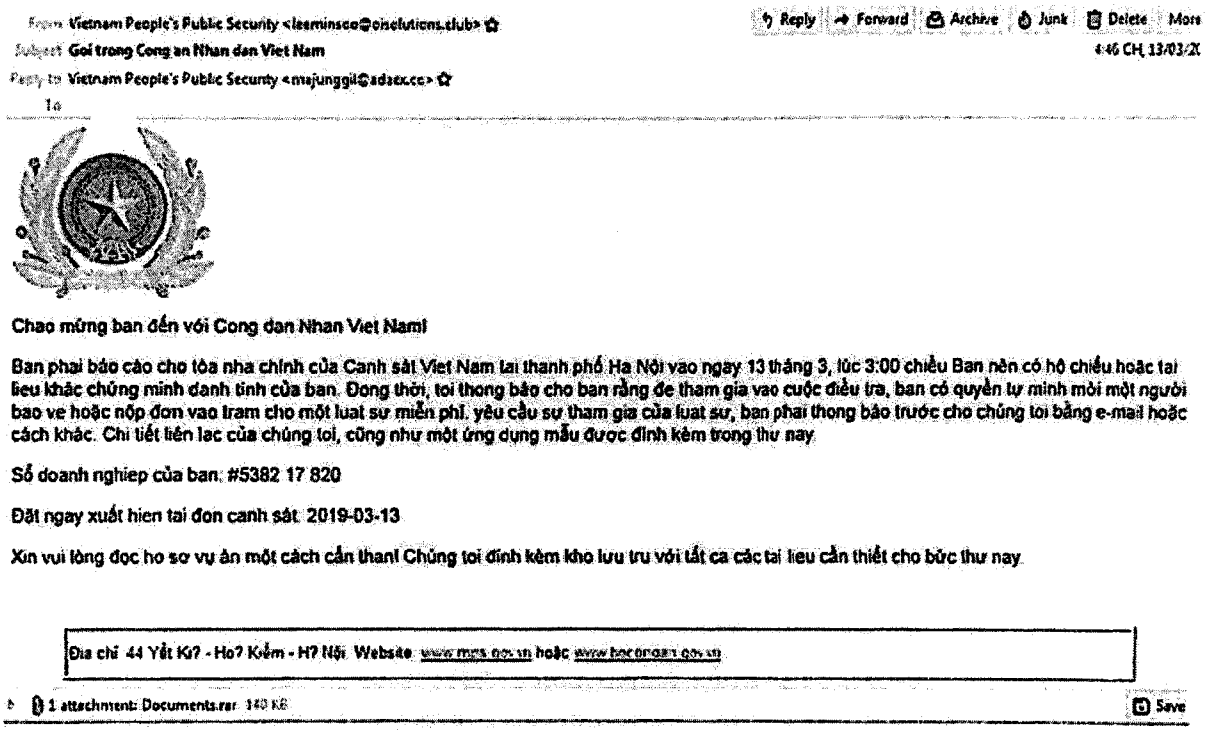
Hà Quốc Trung

PHỤC LỤC

THÔNG TIN VỀ MÃ ĐỘC GANDCRAB v5.2

(Kèm theo Công văn số 60 /TTCNTT-KTHT ngày 18/03/2019 của Trung tâm Công nghệ thông tin)

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 của tệp tin documents.rar

Tìm kiếm tệp tin documents.rar trên máy tính và kiểm tra mã băm tương ứng *(nếu tìm thấy tệp tin chứa mà độc)*

	Mã băm	Ghi chú
MD5	DDCA6B2B2623904A072A5AF0A9E26267	Phiên bản 5.2
SHA1	E081D35048E2DE07BE34C0EAD3B9FD16F6BADB74	Phiên bản 5.2