BỘ THÔNG TIN VÀ TRUYỀN THÔNG
**TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM**

Số: 81 /VNCERT-ĐPƯC
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 15 tháng 3 năm 2019*

HỎA TỐC

Kính gửi:
- Các đơn vị chuyên trách về CNTT, ATTT Văn phòng Trung ương Đảng, Văn phòng Chủ tịch nước, Văn phòng Quốc hội, Văn phòng Chính phủ;
- Các đơn vị chuyên trách về CNTT, ATTT các Bộ, ngành;
- Các Sở Thông tin và Truyền thông;
- Các Tổng công ty, Tập đoàn kinh tế; Tổ chức tài chính và ngân hàng; các doanh nghiệp hạ tầng Viễn thông, Internet, Điện lực, Hàng không, Giao thông vận tải;
- Các thành viên tự nguyện Mạng lưới ứng cứu sự cố ATTT mạng quốc gia.

GandCrab 5.2 là phiên bản mới trong họ Mã độc tống tiền GandCrab lan rộng trên toàn cầu trong hơn một năm qua. Ngày 05/04/2018, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (Trung tâm VNCERT) đã phát hành Công văn số 58/VNCERT-ĐPƯC về việc ngăn chặn kết nối máy chủ điều khiển mã độc GandCrab (phiên bản 1.0 và 2.0) và hiện nay cũng đã hỗ trợ giải mã GandCrab phiên bản 5.1 trở về trước.

Tuy nhiên, hiện nay qua theo dõi không gian mạng, Trung tâm VNCERT phát hiện từ giữa tháng 3/2019 đến nay đang có chiến dịch phát tán Mã độc tống tiền GandCrab 5.2 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 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 môt 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 Quyết định số 05/2017/QĐ-TTg và Thông tư số 20/2017/TT-BTTTT về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc, Trung tâm VNCERT yêu cầu Lãnh đạo đơn vị chỉ đạo các đơn vị thuộc phạm vi

quản lý thực hiện khẩn cấp các việc sau để phòng ngừa, ngăn chặn việc tấn công của mã độc GandCrab 5.2 vào Việt Nam như sau:

1. Theo dõi, ngăn chặn kết nối đến các máy chủ 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 email có chứa các tập tin dạng .doc, .pdf, .zip, rar,… được gửi từ người lạ hoặc nếu email 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 lên nhiều hậu quả nghiêm trọng khác, Trung tâm VNCERT yêu cầu Lãnh đạo các đơn vị nghiêm túc thực hiện lệnh điều phối.

*Mọi chi tiết xin liên hệ Cơ quan Điều phối quốc gia*:

Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam

Địa chỉ: Tầng 5 - Tòa nhà 115 Trần Duy Hưng - Cầu Giấy - Hà Nội;

Điện thoại: 024 3640 4423 số máy lẻ 112;

Đường dây nóng: 0869 100319/ 0888 609399;

Hòm thư điện tử tiếp nhận báo cáo sự cố: ir@vncert.gov.vn.

Trân trọng./.

***Nơi nhận:***
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Thành Hưng (để b/c);
- Giám đốc (để b/c);
- Các Phó Giám đốc (để p/h);
- Các phòng, chi nhánh: KTHT&GS, NCPT, TV&BDNV, CNHCM, CNĐN;
- Lưu: VT, ĐPƯC.

**KT.GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

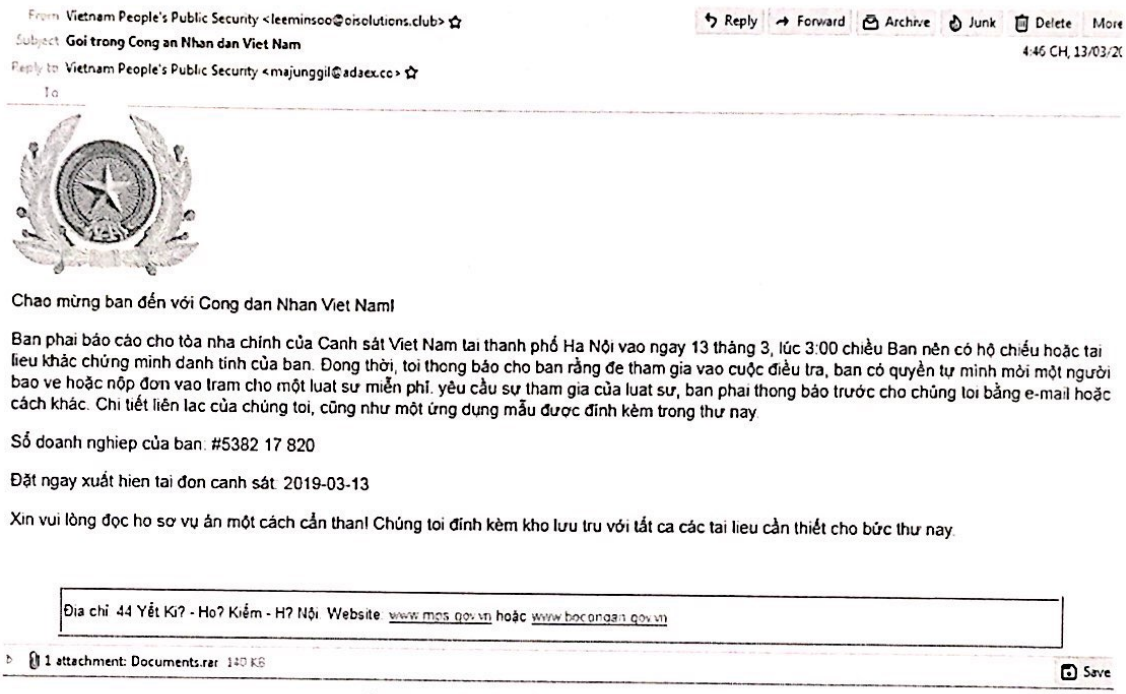
**Nguyễn Khắc Lịch**

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
**TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM**

# PHỤ LỤC
# THÔNG TIN VỀ MÃ ĐỘC GANDCRAB V5.2

*(Kèm theo công văn số 81 /VNCERT-ĐPƯC ngày 15/03/2018 của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam)*

## I. 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*

## II. 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 |

## III. Danh sách mã băm.

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