UBND TỈNH ĐỒNG NAI
SỞ TƯ PHÁP

Số: 800 /STP-VP

V/v triển khai Công văn số 81/VNCERT-DPƯC ngày 15/3/2019 của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam

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

Đồng Nai, ngày 26 tháng 3 năm 2019

Kính gửi:
- Các phòng chuyên môn và tương đương;
- Các đơn vị sự nghiệp trực thuộc Sở.

Sở Tư pháp nhận được Công văn số 437/STTTT-CNTT ngày 21/3/2019 của Sở Thông tin và Truyền thông về việc theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc GandCrab 5.2. Về việc này, Giám đốc Sở Tư pháp yêu cầu:

Trưởng các phòng chuyên môn và tương đương, các đơn vị sự nghiệp trực thuộc Sở triển khai, thực hiện theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc GandCrab 5.2 theo Công văn số 81/VNCERT-DPƯC ngày 15/3/2019 của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam.

Công văn số 81/VNCERT-DPƯC ngày 15/3/2019 của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam về theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc GardCard 5.2 được đăng tải trên mạng thông tin điện tử của Sở Tư pháp tại địa chỉ: http://stp.dongnai.gov.vn, mục văn bản điều hành./.

Nơi nhận:
- Như trên;
- Giám đốc, các Phó Giám đốc Sở;
- Trang TTĐT STP;
- Lưu: VT, VP.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Ngô Văn Toàn

UBND TỈNH ĐỒNG NAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 437 /STTTT-CNTT
V/v theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc GandCrab 5.2

Đồng Nai, ngày 21 tháng 3 năm 2019

Kính gửi:

- Văn phòng Tỉnh ủy;
- Các Sở, Ban, Ngành;
- UBND các huyện, Tx. Long Khánh, Tp. Biên Hòa;
- Các Tổ chức Đoàn thể, Chính trị - Xã hội;
- Đài Phát thanh – Truyền hình Đồng Nai, Báo Đồng Nai, Báo Lao động Đồng Nai.

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 về việc theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc GandCrab 5.2.

Sở Thông tin và Truyền thông thông báo nội dung cảnh báo của Công văn số 81/VNCERT-ĐPƯC nêu trên đến các đơn vị, địa phương để thực hiện, triển khai nhằm đảm bảo an toàn thông tin mạng trên địa bàn tỉnh.

Nội dung chi tiết Công văn trên được đăng tai tại địa chỉ **http://sttt.dongnai.gov.vn**, *mục "AN TOÀN THÔNG TIN"*.

Trân trọng./.

Nơi nhận:
- Như trên;
- P.VHTT các huyện, Tx.Long Khánh, Tp.Biên Hòa;
- Lưu: VT, CNTT.

GIÁM ĐỐC

Lê Hoàng Ngọc

Khu B1 Chung cư Nguyễn Văn Trỗi, đường Nguyễn Ái Quốc, P. Quang Vinh, TP. Biên Hòa - Đồng Nai
TEL: (0613) 810269 – FAX: (0613) 827071

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 Bộ Công an Việt Nam với tiêu đề "*Gọi 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.

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./.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Nguyễn Khắc Lịch

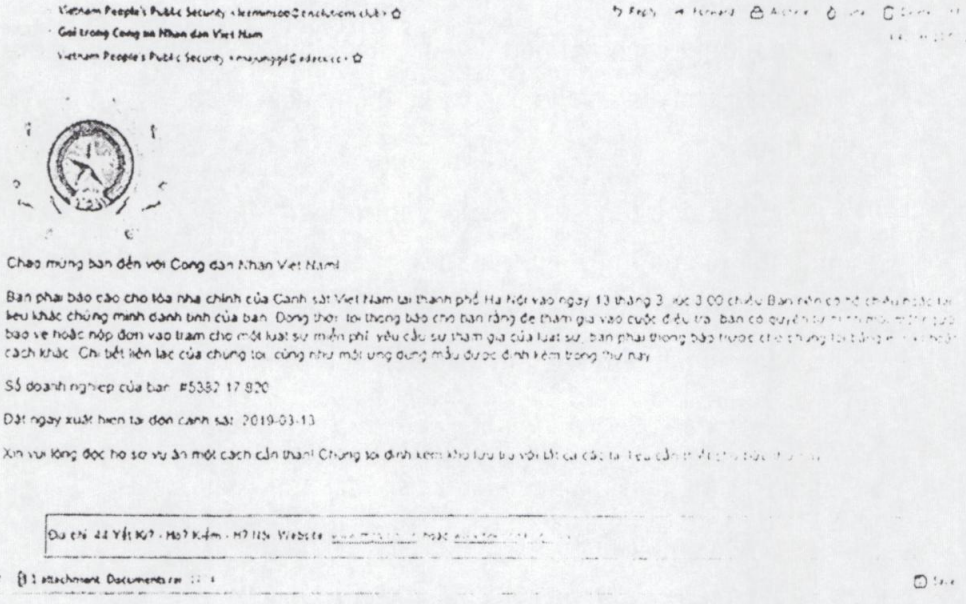
Nơi nhận:
- Như trên;
- Bộ trưởng (để b/c);
- Thứ trưởng Nguyễn Thành Hưng (để b/c);
- Giám đốc (để b/c);
- Các Phó Giám đốc (để p/h);
- Các phòng, chi nhánh: KTHT&GS, NCPT, TV&BDNV, CNHCM, CNĐN;
- Lưu: VT, ĐPƯC.

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 84 /VNCERT-DPUC ngày 15/03/2019 của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam)

I. Hình thức phát tán mã độc.



Chào mừng bạn đến với Cổng dịch vụ công Việt Nam!

Bạn phải báo cáo cho lõa nhà chính của Cảnh sát Việt Nam tại thành phố Hà Nội vào ngày 13 tháng 3 lúc 3:00 chiều. Bạn nên có hộ chiếu hoặc tài liệu khác chứng minh danh tính của bạn. Đồng thời tôi thông báo cho bạn rằng để tham gia vào cuộc điều tra, bạn có quyền thuê luật sư bảo vệ hoặc nộp đơn vào tham chí một luật sư miễn phí. Yêu cầu sự tham gia của luật sư, bạn phải thông báo trước cho chúng tôi bằng một cách khác. Chi tiết liên lạc của chúng tôi cũng như một ứng dụng mẫu được đính kèm trong thư này.

Số doanh nghiệp của bạn: #5382 17 920

Đặt ngày xuất hiện tại đồn cảnh sát: 2019-03-13

Xin vui lòng đọc hồ sơ vụ án một cách cẩn thận! Chúng tôi đính kèm kho lưu trữ với tất cả các tài liệu cần thiết.

Địa chỉ: 44 Yết Kiêu - Hà Nội, Website:

1 attachment: Documents.rar

**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.

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