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

Số: 85 /VNCERT-ĐPƯC
V/v theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc GandCrab

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

Hà Nội, ngày 5 tháng 4 năm 2018

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 Thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia;
- Các Tổng công ty, Tập đoàn kinh tế; các tổ chức Tài chính, Ngân hàng và Chứng khoán; các Doanh nghiệp hạ tầng Internet, Viễn thông, Điện lực, Hàng không, Giao thông vận tải, Dầu khí;
- Các đơn vị thuộc Bộ Thông tin và Truyền thông.

Thực thi nhiệm vụ theo dõi không gian mạng, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) phát hiện đang có chiến dịch phát tán mã độc tống tiền GandCrab tấn công nhiều nước trên thế giới, trong đó có Việt Nam. Mã độc tống tiền GandCrab được phát tán thông qua bộ công cụ khai thác lỗ hổng RIG, khi bị lây nhiễm, toàn bộ các tập tin dữ liệu trên máy người dùng sẽ bị mã hóa và phần mở rộng của tập tin bị đổi thành *.GDCB hoặc *.CRAB, đồng thời mã độc sinh ra một tệp CRAB-DECRYPT.txt nhằm yêu cầu và hướng dẫn người dùng trả tiền chuộc từ 400 - 1.000 USD bằng cách thanh toán qua tiền điện tử DASH 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 vào Việt Nam:

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, … 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 và báo cáo về Cơ quan điều phối quốc gia (VNCERT);

3. Khuyến cáo người sử dụng nâng cao cảnh giác, không mở và click vào các liên kết (link) cũng như các tập tin đính kèm trong email có chứa các tập tin dạng .doc, .pdf, .zip,... 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 nhận được email 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 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

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

Nguyễn Khắc Lịch

Nơi nhận:
- Như trên;
- Bộ trưởng Trương Minh Tuấn (để b/c);
- Thứ trưởng Nguyễn Thành Hưng (để b/c);
- Giám đốc (để b/c);
- Các phòng, chi nhánh: KTHT, NCPT, TVĐT, 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

(Kèm theo công văn số 85 /VNCERT-ĐPƯC ngày 5 /4/2018
của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam)

I. Danh sách các máy chủ điều khiển mã độc GandCrab (C&C Server) cập nhật đến ngày 05/4/2018

TT	Địa chỉ C&C
1	politiaromana.bit
2	malwarehunterteam.bit
3	gdcb.bit

II. Danh sách mã băm (Hash SHA-256)

TT	SHA-256
1	966a0852c8adbea0b7b7aada7c2c851ee642c7bca7da3b29ee143f47ddeb90a5