UBND TỈNH BẮC KẠN
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số 347STTTT-CNTT
V/v theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc GandCrab

Bắc Kạn, ngày 10 tháng 4 năm 2018

Kính gửi:
- Văn phòng HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các Sở, ban, ngành, đoàn thể của tỉnh;
- UBND các huyện, thành phố;

Ngày 09/4/2018, Sở Thông tin và Truyền thông nhận được Công văn số 85/VNCERT-ĐPƯC ngày 05/4/2018 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 GandCarb.

Qua 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.

Để đảm bảo an toàn thông tin cho hệ thống thông tin trên địa bàn tỉnh;Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị thực hiệnkhẩn cấp các việc sau để phòng ngừa, ngăn chặn việc tấn công của mã độc GandCrab 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, ... các thông tin nhận dạng tại phụ lục đính kèm Công văn này;

2. Nếu phát hiện mã độc GandCrab cần nhanh chóng cô lập vùng/máy bị nhiễm và báo cáo về Sở Thông tin và Truyền thông (qua Phòng Công nghệ thông tin) đơn vị thường trực Đội ứng cứu sự cố mạng, máy tính tỉnh Bắc Kạn (BKCERT) để kịp thời xử lý;

3. Khuyến cáo người sử dụng các dịch vụ CNTT 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 thườngvà thông báo

cho bộ phận chuyên trách quản trị hệ thống hoặc đảm bảo an toàn thông tin khi nhận được email nghi ngờ có mã độc.

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, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị nghiêm túc triển khai thực hiện.

Thông tin liên hệ: Phòng Công nghệ thông tin – Sở Thông tin và Truyền thông (đơn vị Thường trực Đội ứng cứu sự cố mạng, máy tính tỉnh Bắc Kạn)

ĐT: 0209 3871 626, email phongcn.tt@backan.gov.vn./.

Nơi nhận:
Gửi bản giấy:
- Các ĐV chưa có phần mềm QLVB&HSCV;
- Lưu: VT.

Gửi bản điện tử:
-Như trên;
- UBND tỉnh (thay báo cáo);
- Trung tâm VNCERT - Bộ TTTT;
- GĐ, PGĐ Sở (ô. Tuyến);
- Phòng CNTT;
- Trung tâm CNTT&TT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Lô Quang Tuyến

PHỤ LỤC
THÔNG TIN VỀ MÃ ĐỘC GRANDCRAB
(Kèm theo Công văn số /STTTT-CNTT ngày10/4/2018
của Sở Thông tin và Truyền thông)

I. Danh sách các máy chủ điều khiển mã độc GrandCrab (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 SIIA-256)

TT	SHA-256
1	966a0852c8adbea0b7b7aada7c2c851ee642c7bca7da3b29eel43f47đđeb90a5