BCĐ UDCNTT TỈNH SƠN LA
ĐỘI ỨNG CỨU SỰ CỐ MẠNG, MÁY TÍNH

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc Lập – Tự Do – Hạnh Phúc

Số: 21 /SONLA-CERT
V/v cảnh báo các ứng dụng phát tán mã độc tống tiền GandCrab

Sơn La, ngày 06 tháng 4 năm 2018

Kính gửi:
- Văn phòng tỉnh ủy, HĐND, UBND tỉnh;
- Các Sở, ban, ngành;
- Công an tỉnh Sơn La;
- Ban Chỉ huy quân sự tỉnh Sơn La;
- UBND các huyện, thành phố;
- Các Hội, Đoàn thể của tỉnh;
- Các thành viên Sơn La - Cert;

Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam đã có Công văn số 85/VNCERT-ĐPƯC ngày 05/4/2018 thông báo về việc hiện tại, 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 lây nhiễm, toàn bộ tập tin 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 cho thiết bị và hệ thống thông tin của đơn vị, Đội trưởng đội Ứng cứu sự cố mạng, máy tính tỉnh Sơn La đề nghị Lãnh đạo các cơ quan 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, bằng cách:

- 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, … các thông tin nhận dạng tại phụ lục đính kèm;

- 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);

- Đối với người dùng, VNCERT cũng khuyến cáo nâng cao cảnh giác, không mở và kích chuột 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

nhiều hậu quả nghiêm trọng khác, yêu cầu thành viên đội SonLa-Cert nghiêm túc thực hiện lệnh điều phối.

Đội Ứng cứu sự cố mạng, máy tính thông báo để các cơ quan, đơn vị, chủ động thực hiện. *(Thông tin hỗ trợ vui lòng liên hệ: Phòng Công nghệ thông tin, Sở Thông tin và Truyền thông tỉnh Sơn La; Đường Hoàng Quốc Việt, TP Sơn La, Tỉnh Sơn La, Điện thoại: 02122.210.468; email: pcntt.stttt@sonla.gov.vn).*

Trân trọng đề nghị các cơ quan, đơn vị quan tâm, thực hiện./.

Nơi nhận:
- Như trên;
- Thường trực UBND tỉnh (để báo cáo);
- Trưởng BCĐ;
- Ban Giám đốc Sở TT&TT;
- Trung tâm CNTT&TT;
- Lưu BCĐ, VT (39b).

ĐỘI TRƯỞNG

Ký bởi: Phạm Quốc Chinh
Email: chinhpq.stttt@sonla.gov.vn
Cơ quan: Sở Thông tin và Truyền thông, Tỉnh Sơn La
Ngày ký: 06.04.2018 17:54:36 +07:00

PHÓ GIÁM ĐỐC SỞ TT&TT
Phạm Quốc Chinh

PHỤ LỤC
THÔNG TIN VỀ MÃ ĐỘC GANDCRAB

(Kèm theo công văn số /STTTT-CNTT ngày 06/4/2018 của Sở Thông tin và Truyền thông)

I. Danh sách các máy chủ điều khiển mã độc GandCrab (C&C Sever) cập nhật đên 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	966a0852c8adbea0b7b7aada7c2c851ee642c7bca7da3b29ee143f47ddeb90a5