UBND TỈNH QUẢNG BÌNH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 233 /STTTT-CNTT
V/v theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc tống tiền GandCrab

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

Quảng Bình, ngày 11 tháng 4 năm 2018

Kính gửi:

- Văn phòng Tỉnh ủy, Văn phòng HĐND tỉnh;
- Các Sở, ban, ngành, đoàn thể cấp tỉnh;
- Các Huyện ủy, Thị ủy, Thành ủy;
- UBND các huyện, thị xã, thành phố;
- Các cơ quan Trung ương đóng trên địa bàn tỉnh.

Sở Thông tin và Truyền thông nhận được thông báo của Trung tâm Ứng cứu sự cố khẩn cấp máy tính Việt Nam (VNCERT) về việc phát hiện đang có chiến dịch phát tán mã độc tống tiến GandCrab tấn công nhiều nước trên thế giới, trong đó có Việt Nam. Mã độc GandCrab rất nguy hiểm, có thể đánh cắp thông tin và mã hóa toàn bộ dữ liệu trên máy tính bị nhiễm. Cách thức phát tán, lây nhiễm và tính năng của mã độc GandCrab như sau:

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 tập tin 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 phòng ngừa, ngăn chặn việc tấn công của mã độc GandCrab, bảo đảm an toàn, an ninh thông tin cho hệ thống máy tính của tổ chức, cá nhân, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị khẩn trương thực hiện:

1. Chỉ đạo bộ phận chuyên trách CNTT, cán bộ quản trị mạng, quản trị máy chủ của cơ quan, đơn vị theo dõi, ngăn chặn kết nối đến các máy chủ điều khiển mã độc GandCrab và cập nhật vào các hệ thống bảo mật như: IDS/IPS, Firewwall... 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 kịp thời cho thường trực Tổ ứng cứu sự cố máy tính của tỉnh.

2. Tổ chức phổ biến, khuyến cáo đối với cán bộ, công chức, viên chức, người lao động của cơ quan, đơn vị và người sử dụng máy tính 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, .dbf, .zip,... được gửi từ người lạ hoặc nếu email được gửi từ người quen nhưng cách đặt tiêu đề hoặc ngôn ngữ khác thường; kịp thời thông báo cho bộ phận chuyên trách CNTT của cơ quan, đơn vị khi nhận được email nghi ngờ.

Quá trình thực hiện nếu có vướng mắc xin liên hệ thường trực Tổ ứng cứu sự cố máy tính của tỉnh (phòng Công nghệ thông tin, Sở Thông tin và Truyền thông; điện thoại: 0232.3851206) để được hướng dẫn, hỗ trợ.

Rất mong được sự quan tâm, phối hợp của các cơ quan, đơn vị./.

Nơi nhận:
- Như trên;
- UBND tỉnh {B/c};
- Lãnh đạo Sở TT&TT;
- Trung tâm CNTT&TT;
- Các thành viên Tổ UCSCMT của tỉnh;
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH QUẢNG BÌNH

Nguyễn Xuân Ngọc

Phụ lục:

THÔNG TIN VỀ MÃ ĐỘC GANDCRAB

(Kèm theo Công văn số 233 /STTTT-CNTT ngày 11 /4/2018 của Sở TT&TT)

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

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

II. Danh sách mã băm (Hash SHA-256)

STT	SHA-256
1	966a0852c8adbea0b7b7aada7c2c851ee642c7bca7da3b29ee143f47ddeb90a5