ỦY BAN NHÂN DÂN **HUYỆN KHÁNH SƠN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 462 / UBND V/v cảnh báo và đề nghị theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc GandCrab	*Khánh Sơn, ngày 13 tháng 4 năm 2018*

Kính gửi:
- Văn phòng HĐND&UBND huyện;
- Các cơ quan, đơn vị, ban, ngành, đoàn thể;
- Các đơn vị sự nghiệp trực thuộc UBND huyện;
- UBND các xã, thị trấn.

Căn cứ Công văn số 589/STTTT-CNTT ngày 10/4/2018 của Sở Thông tin và Truyền thông tỉnh Khánh Hòa về việc cảnh báo và đề nghị theo dõi, ngăn chặn kết nối máy chủ điều khiển, mã độc GandCrab.

Trung tâm VNCERT thông báo việc 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 nhiễm, toàn bộ các tập tin dữ liệu 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 đến 1000 đô la Mỹ (USD) bằng cách thanh toán qua tiền điện tử DASH để giải mã dữ liệu.

Do vậy để chủ động ngăn chặn mã độc trên, UBND huyện Khánh Sơn đề nghị các cơ quan, đơn vị, địa phương khẩn trương thực hiện các nội dung sau:

1. Đối với cán bộ quản trị cổng/trang thông tin điện tử; cán bộ phụ trách CNTT của cơ quan, đơn vị.

- 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,... theo các thông tin nhận dạng mã độc tại *phụ lục đính kèm Công văn này;*

- Trường hợp phát hiện mã độc GandCrab cần nhanh chóng cô lập vùng/ máy bị nhiễm và báo cáo về UBND huyện (thông qua Phòng Văn hóa và Thông tin) để huyện thông báo Đội Ứng cứu sự cố mạng máy tính tỉnh Khánh Hòa phối hợp xử lý.

2. Đối với người dùng cá nhân

- Khuyến cáo người sử dụng nâng cao cảnh giác, không mở và truy cập vào các liên kết (link) cũng như các tập tin đính kèm trong email có chứa các tập tin kể cả trường hợp ở dạng .doc, .pdf, .zip, ... được gửi từ người lạ hoặc email được gửi từ người quen nhưng cách đặt tiêu đề hoặc ngôn ngữ khác thường.

- Khi nhận được email nghi ngờ cần kịp thời thông báo về UBND huyện (thông qua Phòng Văn hóa và Thông tin).

3. Đề nghị các cơ quan, đơn vị, địa phương khẩn trương thông báo nội dung này đến toàn thể cán bộ, công chức, viên chức, người lao động trực thuộc để thực hiện.

Theo cảnh báo của Trung tâm VNCERT, mã độc tống tiền GandCrab rất nguy hiểm, có thể đánh cắp thông tin và mã hóa toàn bộ dữ liệu trên máy tính bị nhiễm. Tin tặc khai thác và tấn công sẽ gây ra nhiều hậu quả nghiêm trọng khác.

Khi phát hiện sự cố mất an toàn thông tin, đề nghị các cơ quan, đơn vị, các địa phương kịp thời báo về UBND huyện (qua Phòng Văn hóa và Thông tin huyện) để huyện thông báo Đội Ứng cứu sự cố mạng máy tính tỉnh Khánh Hòa phối hợp xử lý.

UBND huyện Khánh Sơn đề nghị các cơ quan, đơn vị, địa phương quan tâm triển khai thực hiện./.

Nơi nhận:
- Như trên (VBĐT);
- Lưu: VT, PVHTT.

TM. ỦY BAN NHÂN DÂN
PHÓ CHỦ TỊCH

Bo Bo Thị Yến

Phụ lục

THÔNG TIN VỀ MÃ ĐỘC GANDCRAB

(Kèm theo Công văn số 589/STTTT-CNTT ngày 10/4/2018 của Sở Thông tin và Truyền thông)

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

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

2. Danh sách mã băm (Hash SHA-256)

STT	SHA-256
1	966a0852c8adbea0b7aada7c2c851ee642c7bca7da3b29ee143f47ddeb90a5