| | |
|---|---|
| UBND TỈNH KHÁNH HÒA<br>**SỞ THÔNG TIN VÀ TRUYỀN THÔNG** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**<br>**Độc lập - Tự do - Hạnh phúc** |
| Số: 589/STTTT-CNTT | *Khánh Hòa, ngày 10 tháng 4 năm 2018* |

V/v cảnh báo và đề nghị theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc GandCrab

Kính gửi:
- Các Sở, ban, ngành;
- Ủy ban nhân dân các huyện, thị xã, thành phố;
- Các đơn vị sự nghiệp trực thuộc Ủy ban nhân dân tỉnh.
- Các cơ quan ngành dọc Trung ương.

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 (VNCERT) – Bộ Thông tin và Truyền thông về việc theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc GandCrab.

Tại văn bản nêu trên, 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 phán 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 1.000 đô la Mỹ (USD) bằng cách thanh toán qua tiền điện tử DASH để giải mã dữ liệu.

Để đảm bảo an toàn thông tin mạng trong cơ quan và trên toàn quốc, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị, địa phương thực hiện khuyến cáo tất cả người dùng thực hiện khẩn cấp các công việc sau:

**1.** Đối với các hệ thống thông tin

- 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 đầu mối thường trực Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa.

**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 nếu email được gửi từ người quen nhưng cách đặt tiêu đề hoặc ngôn ngữ khác thường.

- Cần kịp thời thông báo cho bộ phận chuyên trách quản trị hệ thống của cơ quan hoặc đầu mối thường trực Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa khi nhận được email nghi ngờ.

**3.** Đề nghị các cơ quan, đơn vị, địa phương khẩn trương thông báo nội dung văn bản này đến tất cả các cơ quan, đơn vị trực thuộc để tổ chức triển khai 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.

Do vậy, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị, địa phương khẩn trương triển khai thực hiện các nội dung trên và phối hợp chặt chẽ với đầu mối thường trực Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa (*Phòng Công nghệ thông tin – Sở Thông tin và Truyền thông, Điện thoại: 0258.3563533 – Thư điện tử:* cntt.stttt@khanhhoa.gov.vn) trong quá trình theo dõi, ngăn chặn nguy cơ lây nhiễm mã độc.

Trân trọng./.

***Nơi nhận:***
- Như trên (VBĐT);
- UBND tỉnh (VBĐT, để b/c);
- TT VNCERT (VBĐT, để b/c);
- Lưu: VT, CNTT.

**KT.GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**

Ký bởi: Nguyễn Thị Trung Thu
Email: nttthu@khanhhoa.gov.vn
Cơ quan: Sở Thông tin và Truyền thông, Tỉnh

**Nguyễn Thị Trung Thu**

**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 |