SỞ Y TẾ TỈNH KON TUM
TRUNG TÂM Y TẾ ĐĂK GLEI

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

Số: 449/CV-TYĐL
V/v theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc Gand Crab 5.2

Đăk Glei, ngày 3 tháng 04 năm 2019

KHẨN

Kính gửi:
- Các bộ phận trực thuộc TTYT

Thực hiện Công văn số 288/STTTT-CNTT ngày 20/3/2019 của Sở truyền thông thông tin tỉnh Kon Tum về việc theo dõi, ngăn chặn kết nối máy chủ điều khiển mã độc Gand Crab 5.2.

Tại Việt Nam, GandCrab 5.2 được phát tán thông qua thư điện tử giả mạo Bộ Công an Việt Nam với tiêu đề **"Goi trong Cong an Nhan dan Viet Nam"**, có đính kèm tệp **"documents.rar"**. Theo đó, khi người dùng giải nén và mở tệp tin đính kèm, mã độc sẽ được kích hoạt và toàn bộ dữ liệu người dùng bị mã hóa, đồng thời sinh ra môt tệp nhằm yêu cầu và hướng dẫn người dùng trả tiền chuộc từ 400 USD - 1.000 USD bằng cách thanh toán qua đồng tiền điện tử để giải mã dữ liệu.

Thực tế tại địa bàn tỉnh Kon Tum đã có một số cơ quan, ban ngành bị tấn công theo hình thức mã hóa dữ liệu để tống tiền, để phòng ngừa và ngăn chặn việc tấn công bằng mã độc GandCrab 5.2, Trung tâm Y tế huyện Đăk Glei đề nghị các các bộ phận khẩn trương triển khai thực hiện một số nội dung sau:

1. Đối với cán bộ phụ trách CNTT (phòng TCHC):

- Thường xuyên 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… dưới các dạng:

+ Máy chủ điều khiển mã độc:

TT	Địa chỉ C&C	Ghi chú
1	www.kakaocrp.link (IP:107.173.49.208	Phiên bản 5.2

+ Danh sách mã băm (mật mã học):

TT	Địa chỉ C&C	Ghi chú
MD5	DDCA6B2B2623904A072A5À0A9E26267	
SAH1	E081D35048E2DE07BE34C0EAD3B9FD16F6BADB74	

- Nếu phát hiện cần cô lập vùng/máy đã phát hiện.

2. Đối với các bộ phận trực thuộc:

Nâng cao cảnh giác, không mở và click vào các liên kết cũng như các tập tin đính kèm trong email có chứa các tập tin dạng .doc, .pdf, .zip, rar… được gửi từ người lạ hoặc nếu email được gửi từ người quen nhưng cách đặt tiêu đề hoặc ngôn ngữ khác thường; đồng thời thông báo cho cán bộ phụ trách CNTT hoặc đảm bảo an toàn thông tin khi gặp 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 lên nhiều hậu quả nghiêm trọng khác. Do đó, các bộ phận trực thuộc Trung tâm nghiêm túc thực hiện Công văn này./.

Nơi nhận:
- Như trên;
- Lưu: VT, CNTT.

KT. GIÁM ĐỐC

SỞ Y TẾ TỈNH ĐẮK NÔNG
TRUNG TÂM Y TẾ HUYỆN ĐẮK GLONG

PHÓ GIÁM ĐỐC

Lê Đình Thiết