UBND THÀNH PHỐ CẦN THƠ
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 535 /STTTT-TTCNTT&TT
V/v theo dõi, ngăn chặn máy chủ điều khiển mã độc GandCrab

Cần Thơ, ngày 13 tháng 4 năm 2018

Kính gửi:
- Các cơ quan Đảng, Đoàn thể, tổ chức chính trị, xã hội;
- Các đơn vị sở, ban, ngành thành phố;
- Các Trường Cao đẳng, Đại học trên địa bàn thành phố;
- Ủy ban nhân dân quận, huyện.

Sở Thông tin và Truyền thông có nhận được công văn số 85/VNCERT-ĐPƯC ngày 5 tháng 4 năm 2018 của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam về việc theo dõi, ngăn chặn máy chủ điều khiển mã độc GandCrab.

Theo đó, mã độc tống tiền GandCrab đang thực hiện 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 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 để được giải mã dữ liệu.

Để giảm thiểu nguy cơ từ mã độc GandCrab, Sở Thông tin và Truyền thông đề nghị các đơn vị cần thực hiện các công việc như sau:

1. Cập nhật ngay phần mềm diệt virus và bản vá hệ điều hành cho tất cả các máy tính.
2. Sao lưu thường xuyên các dữ liệu quan trọng vào các thiết bị lưu trữ riêng biệt.
3. Nếu phát hiện mã độc GandCrab cần nhanh chóng ngắt kết nối mạng máy bị nhiễm và báo cáo về Đội ứng cứu sự cố an toàn thông tin mạng - Sở Thông tin và Truyền thông để được hỗ trợ.
4. Khuyến cáo người sử dụng 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, .pdf, .zip… được gửi từ người lại hoặc email được gửi từ người quen nhưng cách đặt tiêu đề và nội dung có ngôn ngữ khác thường; đồng thời cần thông báo ngay cho bộ phận chuyên trách CNTT của đơn vị.
5. 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…(nếu có).

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 ra nhiều hậu quả nghiêm trọng khác. Sở Thông tin và Truyền thông đề nghị các đơn vị quan tâm, quán triệt thực hiện theo hướng dẫn như trên.

Mọi chi tiết xin vui lòng liên hệ:

Đội ứng cứu sự cố an toàn thông tin mạng

Địa chỉ: 3A Nguyễn Trãi, Phường An Hội, Quận Ninh Kiều, TP. Cần Thơ.

Điện thoại: 08071213. Di động: 0909.431143 (gặp ông Trần Ngọc Hiền).

Trân trọng./.

Nơi nhận:
- Như trên;
- Lưu VT.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
THÀNH PHỐ CẦN THƠ

Ký bởi: Sở Thông tin và Truyền thông thành phố Cần Thơ
Email: sotttt@cantho.gov.vn
Cơ quan: UBND thành phố Cần Thơ
Thời gian ký:13.04.2018 10:21:26 +07:00

Nguyễn Hữu Thanh Bình