UBND TỈNH NINH THUẬN
SỞ GIÁO DỤC VÀ ĐÀO TẠO

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

Số: 957/SGDĐT-VP

Ninh Thuận, ngày 12 tháng 4 năm 2018

V/v cảnh báo, ngăn chặn kết nối máy chủ điều khiển mã độc GandCrab.

Kính gửi:
- Phòng Giáo dục và Đào tạo các huyện, thành phố;
- Các đơn vị trực thuộc Sở.

Căn cứ Công văn số 85/VNCERT-ĐPƯC ngày 05/4/2018 của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam về việc cảnh báo, ngăn chặn kết nối máy chủ điều khiển mã độc GandCrab;

Tiếp nhận Công văn số 569/STTTT-CNTT ngày 09/4/2018 của Sở Thông tin và Truyền thông về cảnh báo, ngăn chặn kết nối máy chủ điều khiển mã độc GandCrab,

Theo ghi nhận của Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) 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 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 tệp 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..

Nhằm phòng ngừa, ngăn chặn việc tấn công của mã độc GandCrab và đảm bảo an toàn cho người sử dụng trong truy cập internet, Sở Giáo dục và Đào tạo yêu cầu các đơn vị, cán bộ, công chức, viên chức Ngành Giáo dục và Đào tạo khẩn cấp thực hiện các công việc sau:

1. Nhân viên, chuyên trách CNTT thuộc Phòng Giáo dục và Đào tạo huyện, thành phố; các đơn vị trực thuộc Sở:

- 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 phụ lục các thông tin nhận dạng của VNCERT (đính kèm công văn này);

- Thực hiện sao lưu dữ liệu trên các hệ thống phần mềm dùng chung ra các thiết bị lưu trữ độc lập như máy chủ backup dữ liệu, ổ cứng di động, DVD,…

- Thực hiện cô lập vùng/máy bị nhiễm và báo cáo về Sở Giáo dục và Đào tạo hoặc Sở Thông tin và Truyền thông hoặc VNCERT.

2. Cán bộ, công chức, viên chức Ngành Giáo dục:

- Nâng cao cảnh giác, không mở hoặc nhấp chuột vào các liên kết (link) cũng như các tập tin đính kèm trong thư điện tử chứa các tập tin có định dạng đuôi

.doc, .pdf, .zip, … được gửi từ hộp thư điện tử của người lạ hoặc thư điện tử được gửi từ người quen nhưng cách đặt tiêu đề hoặc ngôn ngữ khác thường;

- Thực hiện sao lưu các dữ liệu quan trọng sang các thiết bị lưu trữ độc lập như đĩa DVD, ổ cứng di động, USB,…

- Nếu phát hiện hoặc nghi ngờ máy nhiễm mã độc, chủ động cô lập máy tính (rút dây mạng, tắt nguồn máy tính) và thông báo cho bộ phận chuyên trách, quản trị hệ thống để xử lý.

3. Đầu mối liên hệ hỗ trợ:

Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT

- Địa chỉ: Tầng 5, Tòa nhà 115 Trần Duy Hưng, Cầu Giấy, Hà Nội;

- Điện thoại: 04 3640 4423 số máy lẻ 112;

- Đường dây nóng: 0934 424 009;

- Hòm thư điện tử tiếp nhận báo cáo sự cố: ir@vncert.gov.vn.

Sở Thông tin và Truyền thông tỉnh Ninh Thuận

- Địa chỉ: 17 Nguyễn Trãi, phường Kinh Dinh, Tp. Phan Rang - Tháp Chàm, Ninh Thuận;

- Điện thoại: 0259.3922753;

- Thư điện tử: sotttt@ninhthuan.gov.vn;

Sở Giáo dục và Đào tạo tỉnh Ninh Thuận

- Địa chỉ: 18 Lê Hồng Phong, phường Mỹ Hương, Tp. Phan Rang - Tháp Chàm, Ninh Thuận;

- Điện thoại: 0259.3832424;

- Thư điện tử: sogddt@ninhthuan.gov.vn

hoặc phongcntt.soninhthuan@moet.edu.vn

Đề nghị Trưởng phòng Giáo dục và Đào tạo các huyện, thành phố; Các đơn vị trực thuộc Sở; Các phòng chức năng thuộc Sở khẩn trương triển khai các biện pháp trên nhằm hạn chế việc lây lan, giảm thiểu nguy cơ nhiễm mã độc có thể xảy ra./.

Nơi nhận:
- Như trên;
- GĐ, PGĐ Sở;
- Các phòng chức năng thuộc Sở;
- Cổng TTĐT Ngành;
- Phòng GDTrH: Trần Văn Linh;
- Lưu: VT, VP.HTHG.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH NINH THUẬN

Lê Bá Phương

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM

PHỤ LỤC
THÔNG TIN VỀ MÃ ĐỘC GANDCRAB

(Kèm theo công văn số 85 /VNCERT-ĐPƯC ngày 5/4/2018
của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam)

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

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

II. Danh sách mã băm (Hash SIIA-256)

TT	SHA-256
1	966a0852c8adbea0b7b7aada7c2c851ee642c7bca7da3b29ee143f47ddeb90a5