UBND TỈNH LAI CHÂU
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: 767 /STTTT-BCVTCNTT
V/v cảnh báo nguy cơ lây nhiễm mã độc cho các mạng CNTT của cơ quan Đảng, Nhà nước

Lai Châu, ngày 12 tháng 9 năm 2018

Kính gửi:
- Các Sở, Ban, Ngành, Đoàn thể tỉnh;
- UBND huyện , Thành phố.

Trong thời gian vừa qua, qua phân tích và theo dõi đã phát hiện một số mạng CNTT, máy tính (máy chủ và máy trạm) của cơ quan Đảng, Nhà nước nhiễm mã độc và có kết nối đến các máy chủ điều khiển từ xa, các máy chủ này nằm tại các quốc gia như Nga, Mỹ, Trung Quốc… Các loại mã độc phát hiện được chủ yếu là các loại mã độc phổ biến như: Trojan downloader, keylogger, malware-gen… và một số loại mã độc được chèn, tiêm nhiễm trong các tập tin văn bản (.doc, .xls) có đính kèm gửi qua thư điện tử nhằm vào các máy tính trong hệ thống mạng để lấy nhiễm, đánh cắp thông tin từ người dùng trong hệ thống. Ngoài ra, có một số loại mã độc mới khai thác lỗ hổng của ứng dụng văn bản Microsoft Office, khai thác lỗ hổng của hệ điều hành Windows cũng được phát tán và lây nhiễm, thông qua đính kèm các tệp tin văn bản.

Để hạn chế nguy cơ lây nhiễm mã độc, Sở Thông tin và Truyền thông đề nghị các cơ quan Đảng, Nhà nước cần thực hiện các biện pháp sau:

1. Cài đặt, sử dụng phần mềm diệt virus chính hãng, có bản quyền và thường xuyên cập nhật phần mềm diệt virus;

2. Cập nhật các bản vá chính thức của hệ điều hành. Kiểm tra và bật tính năng tường lửa bảo vệ của hệ điều hành đã được cài đặt trên máy tính. Xem xét, lưu ý các hiện tượng và cảnh báo bất thường trên máy tính để có biện pháp xử lý kịp thời;

3. Khi nhận thư điện tử phải kiểm tra nguồn gửi rõ ràng, các tập tin đính kèm phù hợp với nội dung thư và người gửi thư trước khi mở hay tải tập tin về máy tính. Những tập tin đính kèm trong thư điện tử, bao gồm cả các tập tin nén như file .zip cần được lưu vào ổ đĩa và rà quét trước khi được mở ra. Không gửi hoặc nhận một số loại tập tin có các đuôi tệp tin là .exe qua thư điện tử. Không mở các tập tin với phần mở rộng có khả năng kết hợp với phần mềm độc hại (Ví dụ: .bat, .exe, .pif, .vbs...);

4. Sử dụng Internet có chọn lọc, không vào các trang web lạ, không bấm vào các đường liên kết, biểu tượng quảng cáo không rõ và không truy cập vào các popup trên trình duyệt mà cảm thấy nghi ngờ hoặc có dấu hiệu bất thường;

5. Cập nhật các bản vá của ứng dụng Microsoft Office;

6. Hạn chế kết nối các máy tính, thiết bị ngoại vi (USB, ổ cứng, thẻ nhớ...) chưa được kiểm soát vào hệ thống mạng LAN của đơn vị, nếu phải kết nối yêu cầu dùng phần mềm rà quét các thiết bị trước khi sử dụng;

7. Không sử dụng phần mềm được cung cấp bởi các tổ chức không rõ nguồn gốc, hạn chế sử dụng hộp thư miễn phí trong trao đổi công vụ;

8. Thường xuyên đổi mật khẩu các tài khoản trong trao đổi công vụ, đảm bảo độ mạnh của mật khẩu (trên 8 ký tự, bao gồm ký tự thường, ký tự hoa, ký tự số và ký tự đặc biệt);

9. Tiến hành các biện pháp lưu trữ, sao lưu (backup) dữ liệu quan trọng ra khỏi máy tính;

10. Thường xuyên rà quét, đánh giá, xử lý mã độc định kỳ để kịp thời xử lý.

Trên đây là những biện pháp hạn chế nguy cơ lây nhiễm mã độc cho các mạng CNTT của cơ quan Đảng, Nhà nước, khuyến nghị các đơn vị triển khai, thực hiện. Trường hợp cần hướng dẫn, liên hệ Phòng Bưu chính - Viễn thông - Công nghệ thông tin, điện thoại 02313798798 hoặc đồng chí Bùi Thị Lan, điện thoại: 01679122000.

Sở Thông tin và Truyền thông đề nghị Lãnh đạo quý cơ quan quan tâm triển khai, thực hiện./.

Nơi nhận:
- Như trên;
- Tỉnh ủy (b/c);
- UBND tỉnh (b/c);
- Phòng BCVTCNTT, Cổng TTĐT;
- Trung tâm CNTT & TT;
- Lưu: VT.

- Vhoá TT, các cơ quan
- Đài TTTH huyện thị xã thành phố

GIÁM ĐỐC

SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Quốc Luân