SỞ THÔNG TIN VÀ TRUYỀN THÔNG CAO BẰNG
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 03 /TTCNTTTT-KTCN
V/v Cảnh báo nguy cơ mã độc mã hoá dữ liệu tấn công vào hệ thống thông tin của các cơ quan, tổ chức trên địa bàn tỉnh Cao Bằng

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

Cao Bằng, ngày 07 tháng 01 năm 2021

Kính gửi:

- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các sở, ngành, UBND các huyện, thành phố;
- Các đơn vị sự nghiệp công lập, doanh nghiệp nhà nước.

Nhằm tăng cường bảo đảm an toàn, an ninh mạng, không để bị động, bất ngờ với mọi tình huống tấn công mạng và phát tán thông tin xấu độc, lây nhiễm mã độc gây mất an toàn thông tin trên địa bàn tỉnh. Qua công tác theo dõi và rà soát an toàn thông tin, Trung tâm Công nghệ thông tin và Truyền thông – Sở Thông tin và Truyền thông cảnh báo nguy cơ mã độc mã hoá dữ liệu tấn công vào hệ thống thông tin của các cơ quan, tổ chức, cụ thể như sau:

Ngày 31/12/2020, Trung tâm ghi nhận có mã độc mã hoá dữ liệu (Ransomeware) tấn công vào một số máy chủ chạy hệ điều hành Window Server trên địa bàn tỉnh, mã độc đã mã hoá toàn bộ dữ liệu của máy tính và thông báo yêu cầu trả tiền để được giải mã dữ liệu đã bị mã hóa. Đây là dạng Ransomeware Globeimposter 2.0, một loại mã độc mã hóa dữ liệu đòi tiền chuộc, mã độc này được đóng gói trong các tệp tin có thể qua mặt được một số phần mềm diệt virus và hiện tại chưa có công cụ giải mã loại ransomware này.

Mã độc này lây nhiễm chủ yếu qua các cách thức chủ yếu sau:

- Tích hợp với các ứng dụng, phần mềm không rõ nguồn gốc, phần mềm bẻ khoá...

- Các file đính kèm thư rác, thư giả mạo.

- Từ các trang web cung cấp dịch vụ lưu trữ miễn phí, website giả mạo, các popup quảng cáo, website chứa nội dung không lành mạnh.

- Tấn công mạng có chủ đích (APT).

Để đảm bảo an toàn thông tin cho hệ thống thông tin tại đơn vị, Trung tâm Công nghệ thông tin và Truyền thông kính đề nghị các cơ quan, đơn vị chỉ đạo bộ phận chuyên môn thực hiện một số nội dung sau :

1. Theo dõi và ngăn chặn mạng của đơn vị kết nối đến IP: 89.39.107.61 (đây là máy chủ phát tán, điều khiển, mã độc).

2. Rà soát lại toàn bộ hệ thống thông tin, máy tính của cơ quan, đơn vị, thực hiện kiểm tra, đánh giá để chủ động phát hiện và xử lý kịp thời các lỗ hổng bảo mật. Thường xuyên cập nhật bản vá hệ điều hành, bản vá lỗ hổng bảo mật cho các máy chủ, máy tính, phần mềm nhất là các lỗ hổng để điều khiển từ xa như: CVE 2020-0796, CVE-2020-17022, CVE-2020-16898, CVE-2020-1374, CVE-2020-1301...

3. Tăng cường theo dõi giám sát đồng thời thường xuyên theo dõi kênh cảnh báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

4. 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 lạ hoặc nếu email được gửi từ người quen nhưng cách đặt tiêu đề hoặc ngôn ngữ khác thường, cần thông báo cho bộ phận chuyên trách quản trị hệ thống hoặc đảm bảo an toàn thông tin khi nhận được email nghi ngờ.

5. Không sử dụng các công cụ, phần mềm bẻ khoá, không rõ nguồn gốc.

6. Không truy cập các trang web cung cấp dịch vụ lưu trữ miễn phí, website giả mạo, không click vào các popup quảng cáo...

7. Cài đặt phần mềm diệt virus bản quyền và thường xuyên cập nhật trên toàn bộ máy tính của đơn vị.

8. Cần triển khai lắp đặt một số thiết bị tối thiểu để đảm bảo an toàn thông tin cho hệ thống máy chủ như: Hệ thống tường lửa Firewall, Hệ thống phát hiện, phòng chống xâm nhập IDS/IPS, Hệ thống phòng chống DOS/DDOS, proxy, Application firewall.

Trong trường hợp cần hỗ trợ có thể liên hệ đầu đầu mối ứng cứu sự cố máy tính tỉnh Cao Bằng:

Trung tâm Công nghệ thông tin và Truyền thông Cao Bằng.

Địa chỉ: Số 009, Hoàng Văn Thụ, Hợp Giang, thành phố Cao Bằng,

Điện thoại: 0206.3955.899. Email: cbitc@caobang.gov.vn./.

Nơi nhận:
- Như trên;
- Sở TT&TT (để b/c);
- Phòng BCVT-CNTT;
- Lưu VT, KTCGCN.

GIÁM ĐỐC

Triệu Đình Thăng