

**ỦY BAN NHÂN DÂN
TỈNH TUYÊN QUANG**

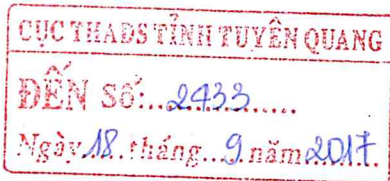
**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc**

Số: 2901 /UBND-THCB

Tuyên Quang, ngày 15 tháng 9 năm 2017

V/v tăng cường bảo đảm an toàn
thông tin trước sự kiện APEC 2017

Kính gửi:



- Các Sở, ban, ngành;
- Ủy ban nhân dân huyện, thành phố;
- Các tổ chức chính trị xã hội;
- Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet.

Việt Nam là nước chủ nhà Năm APEC 2017, chủ trì tổ chức các cuộc họp quan trọng tại nhiều địa phương trên khắp cả nước, đặc biệt là Tuần lễ Hội nghị cấp cao diễn ra vào trung tuần tháng 11 tại Đà Nẵng.

+ Thời gian vừa qua, tình hình an toàn thông tin trong nước tiếp tục diễn biến phức tạp. Các cơ quan chức năng của Bộ Thông tin và Truyền thông ghi nhận dấu hiệu hoạt động trở lại của các nhóm đối tượng đã từng thực hiện một số cuộc tấn công mạng vào Việt Nam trước đây, thông qua việc thay đổi, chuyển sang sử dụng hạ tầng mới, thêm mới nhiều hệ thống máy chủ điều khiển tấn công mạng từ xa (C&C servers), phương thức tấn công mạng và các tên miền sử dụng làm máy chủ điều khiển:

a) Phương thức tấn công mạng

Tấn công có chủ đích (APT), phương thức thực hiện chính vẫn là gửi thư điện tử giả mạo liên quan tới các chủ đề nhạy cảm được nhiều người quan tâm như: Chủ đề hoạt động kinh tế của ASEAN, APEC, Biển Đông ...

Cục An toàn thông tin Bộ Thông tin và Truyền thông đã ghi nhận một số trường hợp mã độc khai thác lợi dụng chính các phần mềm diệt vi-rút phổ biến để thực hiện lây nhiễm. Người nhận thư điện tử chỉ mới thực hiện thao tác quét tệp tin bằng phần mềm diệt vi-rút để kiểm tra mã độc mà chưa cần mở tệp tin độc nội dung cũng bị lây nhiễm mã độc.

Một số ví dụ về các tệp tin được sử dụng để phát tán mã độc được ghi nhận như sau:

Đảm bảo an toàn APEC 2017.doc

Báo cáo cho cuộc gặp Tổng Bí thư tháng 1 năm 2017.doc

Kế hoạch kiểm tra khảo sát Quyết định 221 - BBT.doc

Biểu mẫu kiểm tra, giám sát- năm 2017(sử dụng tại các chi bộ).doc

Tài liệu phòng chống DBHB.doc

CV950-BTCTW tương đương trình độ cao cấp lý luận chính trị.doc

De tai cuong quoc bien TQ.doc

...

b) Danh sách một số tên miền được sử dụng để làm máy chủ điều khiển

(Có danh sách kèm theo)

Đáng chú ý, một số tên miền giả mạo, dễ làm người sử dụng liên tưởng đến các cơ quan, tổ chức có uy tín của Việt Nam như:

dcsvn.org

news.vietnannet.com

news.phapluats.com

vnnexpress.org

vietnamplos.com

dulichvietnam.net

...

Nhằm tăng cường bảo đảm an toàn thông tin, đặc biệt trước thời điểm diễn ra Tuần lễ Hội nghị cấp cao APEC 2017,

Ủy ban nhân dân tỉnh yêu cầu:

1. Các Sở, ban, ngành, Ủy ban nhân dân các huyện, thành phố

- Tiếp tục thực hiện sự chỉ đạo của Ủy ban nhân dân tỉnh tại Văn bản số 150/UBND-THCB ngày 18/01/2017, 738/UBND-THCB ngày 22/3/2017 về tăng cường công tác đảm bảo an ninh, an toàn thông tin.

- Tổ chức rà soát, kiểm tra, thực hiện đầy đủ, kịp thời các quy định về đảm bảo an toàn thông tin nói chung, chú trọng bảo đảm an toàn thông tin cho trang/cổng thông tin điện tử và hệ thống thư điện tử theo hướng dẫn tại Công văn số 430/BTTTT-CATTT ngày 09/02/2015 của Bộ Thông tin và Truyền thông; tăng cường bảo đảm an toàn thông tin cho hạ tầng mạng nội bộ, mạng không dây phục vụ hoạt động tại đơn vị.

- Rà soát, tăng cường bảo đảm an toàn thông tin cho toàn bộ màn hình, thiết bị hiển thị, thiết bị truyền thông đa phương tiện công cộng; đặc biệt tại các địa điểm diễn ra các cuộc họp, hội nghị ...

- Cử đầu mối phối hợp với Sở Thông tin và Truyền thông để xử lý kịp thời khi xảy ra sự cố mất an toàn thông tin.

2. Sở Thông tin và Truyền thông

- Chủ trì, phối hợp với các cơ quan đơn vị chủ động rà soát, triển khai các giải pháp đảm bảo an toàn thông tin cho các hệ thống thông tin; đặc biệt là Cổng thông tin điện tử, hệ thống thư điện tử.

- Làm đầu mối nắm bắt, tiếp nhận, xử lý khi có sự cố mất an toàn thông tin xảy ra trên địa bàn tỉnh (thông tin liên hệ đội ứng cứu sự cố sở Thông tin và truyền thông: 0948536888 hoặc 0987320203, thongtintt@tuyenquang.gov.vn).

- Phối hợp chặt chẽ với Cục An toàn thông tin Bộ Thông tin và Truyền thông kiểm tra cũng như nhận phương án hỗ trợ kỹ thuật nhằm ngăn chặn kịp thời các hạ tầng tấn công có chủ đích APT mà Cục An toàn thông tin đang giám sát theo dõi.

3. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet

- Tăng cường công tác giám sát thường xuyên để kịp thời phát hiện và ngăn chặn các hành vi tấn công mạng gây mất an toàn thông tin trên toàn mạng

lưới viễn thông, Internet mà đơn vị quản lý trước và trong Tuần lễ Hội nghị cấp cao APEC 2017.

- Có phương án, kế hoạch để bảo đảm an toàn thông tin, đặc biệt là tổ chức dự phòng để duy trì tính sẵn sàng cho các dịch vụ viễn thông và Internet mà đơn vị cung cấp.

- Phối hợp kịp thời với Sở Thông tin và Truyền thông (đội ứng cứu sự cố nói trên) và Cục An toàn thông tin nắm bắt và xử lý các mối nguy hại thường trực đang tồn tại, tiếp tục theo sát, xử lý các diễn biến mới.

Thông tin liên hệ của Cục An toàn thông tin khi cần trao đổi và hỗ trợ tư vấn, xử lý:

+ Thư điện tử: ais@mic.gov.vn

+ Điện thoại đường dây nóng: 0989344430 hoặc 0922556666.

Ủy ban nhân dân tỉnh yêu cầu các cơ quan, đơn vị nghiêm túc triển khai, thực hiện./.

Nơi nhận: 

- Như trên (thực hiện);
- Chủ tịch UBND tỉnh (báo cáo);
- PCT UBND tỉnh Nguyễn Hải Anh;
- CVP, các PCVP UBND tỉnh;
- Lưu VT, TH-CB (Tùng CNTT).

**KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**



Nguyễn Hải Anh

