UBND TỈNH GIA LAI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 225/STTTT-CNTT
V/v hướng dẫn khắc phục và xử lý sự cố mất an toàn thông tin mạng trên địa bàn tỉnh

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

Gia Lai, ngày 26 tháng 02 năm 2020

Kính gửi:
- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn Đại biểu Quốc hội tỉnh;
- Văn phòng Hội đồng nhân dân tỉnh;
- Văn phòng Ủy ban nhân dân tỉnh;
- Văn phòng Ủy ban MTTQ Việt Nam tỉnh;
- Bộ Chỉ huy Quân sự tỉnh Gia Lai;
- Công an tỉnh Gia Lai;
- Các Sở, ban, ngành thuộc tỉnh;
- Các Hội, Đoàn thể của tỉnh;
- Ủy ban nhân dân các huyện, thị xã, thành phố;
- Các doanh nghiệp Viễn thông trên địa bàn tỉnh.

Sở Thông tin và Truyền thông (TT&TT) nhận được thông báo của Trung tâm Giám sát an toàn không gian mạng Quốc gia thuộc Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc phát hiện địa chỉ IP của một số cơ quan, đơn vị sử dụng đang bị tham gia mạng lưới Botnet, nhiễm virus. Do đó, Sở TT&TT đề nghị các cơ quan, đơn vị khoanh vùng, gỡ bỏ mã độc khỏi mạng Botnet, nhiễm virus.

Thông tin về các địa chỉ IP bị sử dụng tham gia mạng lưới Bonet, nhiễm virus cụ thể như sau:

STT	Địa chỉ IP bị nhiễm	Địa chỉ IP đích kết nối mã độc	Mạng botnet/virus	Thời gian phát hiện	Cơ quan, đơn vị sử dụng IP
1	113.161.25.3	72.26.218.74	Avalanche	23/02/2020	Đài Phát thanh - Truyền hình tỉnh
2	113.161.25.55	107.6.74.81	Avalanche	23/02/2020	UBND huyện Đak Pơ
3	113.161.25.225	184.105.192.2	Avalanche	22/02/2020	UBND huyện Ia Pa
4	118.69.109.243	72.26.218.74	Avalanche	19/02/2020	Thanh tra tỉnh
5		35.229.93.46		23/02/2020	
6	118.69.109.244	35.231.151.7	Avalanche	19/02/2020	Sở Tư pháp
7		35.229.93.46		23/02/2020	
8	117.3.139.132	184.105.192.2	Avalanche	23/02/2020	Phòng Giáo dục và Đào tạo thị xã Ayun Pa
9	113.161.24.71	184.105.192.2	Avalanche	23/02/2020	UBND huyện Ia Grai
10	117.3.100.95	107.6.74.81	Avalanche	19/02/2020	Văn phòng Tỉnh ủy
11		208.100.26.234	Lethic	22/02/2020	
12	113.161.24.53	208.100.26.234	Lethic	25/02/2020	UBND huyện Kông

13	113.161.24.53	72.26.218.74	Avalanche	23/02/2020	Chro
14	113.161.22.2	104.17.244.81	Wannacry	19/02/2020	Sở Nông nghiệp và Phát triển nông thôn
15	117.3.65.7	104.17.244.81	Wannacry	19/02/2020	Sở Tài chính
16	113.161.24.92			25/02/2020	
17	117.3.64.216	184.105.192.2	Avalanche	23/02/2020	Văn phòng Hội đồng nhân dân tỉnh
18	113.161.22.17	72.26.218.74	Avalanche	25/02/2020	Sở Tài nguyên và Môi trường

Sở TT&TT đề nghị các cơ quan, đơn vị kiểm tra lại địa chỉ IP của đơn vị mình và xử lý ngay khi nhận được thông báo này. Cách thức xử lý như sau:

1. Khoanh vùng nhằm tìm kiếm máy tính trong hệ thống máy tính của cơ quan đơn vị đang bị nhiễm mã độc. Cài đặt phần mềm chống virus để quét máy tính bị nhiễm. Tham khảo hướng dẫn tại: Công văn số 385/STTTT-CNTT ngày 15/5/2017 của Sở Thông tin và Truyền thông tỉnh Gia Lai về việc cảnh báo và xử lý Virus Wannacry *(có gửi kèm theo)*.

2. Cập nhật thường xuyên các bản vá cho hệ điều hành và phần mềm chống virus.

3. Sao lưu dữ liệu quan trọng trên máy chủ; rà soát toàn bộ máy chủ của đơn vị, hạn chế tối đa việc mở cổng dịch vụ Remote Desktop. Trong trường hợp cần sử dụng phải thiết lập các chính sách bảo mật như: sử dụng mạng riêng ảo (VPN), giới hạn IP truy cập, tài khoản được phép truy cập, chính sách mật khẩu mạnh (mật khẩu có tối thiểu 8 ký tự, có đầy đủ chữ hoa, chữ thường, số và ký tự đặc biệt).

Kiểm tra các dịch vụ sử dụng giao thức UDP, hạn chế tối đa việc mở các cổng dịch vụ sử dụng giao thức UDP. Trong trường hợp sử dụng phải thường xuyên theo dõi và cập nhật bản vá lỗ hổng bảo mật cho dịch vụ, đồng thời cấu hình cứng hóa dịch vụ, hạn chế tối đa truy cập đến và đi liên quan đến địa chỉ/dải địa chỉ không cần thiết.

4. Sử dụng tường lửa (firewall) hoặc các thiết bị có chức năng tương tự để chặn các kết nối đến các máy chủ có địa chỉ IP đích kết nối theo danh sách ở trên.

Kiểm tra và xử lý các thiết bị trong toàn bộ hệ thống mạng nếu có dấu hiện kết nối đến các tên miền độc hại như:

STT	**Tên miền/IP**
1	disorderstatus.ru
2	differentia.ru
3	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
4	atomictrivia.ru
5	soplifan.ru
6	somicrososoft.ru
7	morphed.ru
8	awjapmnak.info
9	www.cityofangelsmagazine.com
10	a.deltaheavy.ru

11	www.corpnox-technologie.fr
12	3851e33b032827cade4afe6d3f58eba1.online
13	bharatisangli.in

5. Giao cán bộ chuyên trách CNTT, thành viên Đội ứng sự cố an toàn thông tin tỉnh (hoặc đơn vị, bộ phận chuyên trách CNTT) thường xuyên, giám sát hệ thống để phát hiện sớm, kịp thời phản ứng các hành vi dò quét/tấn công mạng và cập nhật bản vá cho các lỗ hổng bảo mật, đảm bảo tình hình an toàn thông tin của đơn vị.

Khi phát hiện bị tấn công mã hoá dữ liệu liên hệ với đơn vị cung cấp dịch vụ bảo mật/giải mã dữ liệu gần nhất để có biện pháp khôi phục dữ liệu hoặc liên hệ phòng Nghiệp vụ (Trung tâm CNTT&TT tỉnh Gia Lai), số điện thoại: 02693.512.282 (di động: 0363.675.110) gặp đồng chí Nguyễn Tiến Cường để được hướng dẫn chi tiết.

Sở Thông tin và Truyền thông Gia Lai đề nghị cơ quan, đơn vị, địa phương quan tâm thực hiện nhằm bảo đảm an toàn thông tin mạng trên địa bàn tỉnh./.

Nơi nhận:
- Như trên;
- UBND tỉnh (báo cáo);
- Cục ATTT – Bộ TT&TT;
- Trung tâm Công nghệ thông tin và Truyền thông (phối hợp thực hiện);
- Lưu: VT, P.CNTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH GIA LAI

Đặng Quang Khanh

Sở Thông tin và Truyền thông
Tỉnh Gia Lai
24.02.2020
16:15:16 +07:00