SỞ Y TẾ TỈNH AN GIANG
TRUNG TÂM Y TẾ KIÊN HẢI

Số: 202 /TTYT-TCHC

V/v thông báo tình hình hoạt động tấn công mạng, gián điệp mạng tại Việt Nam thời gian qua

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

Kiên Hải, ngày 30 tháng 7 năm 2025

Kính gửi: Phòng, khoa và các Trạm Y tế.

Thực hiện Công văn số 524/SYT – CNTT ngày 29 tháng 7 năm 2025 của Sở Y tế tỉnh An Giang về việc thông báo tình hình hoạt động tấn công mạng, gián điệp mạng tại Việt Nam thời gian qua.

Trung tâm Y tế Kiên Hải đề nghị lãnh đạo phòng, khoa và các Trạm Y tế triển khai, quán triệt nội dung Công văn số 230/UBND-KGVX ngày 28/7/2025 của UBND tỉnh An Giang về việc thông báo tình hình hoạt động tấn công mạng, gián điệp mạng tại Việt Nam thời gian qua, đến toàn thể viên chức và người lao động thuộc quyền quản lý biết và thực hiện.

(đính kèm công văn)

Nhận được công văn này đề nghị lãnh đạo phòng, khoa và các Trạm Y tế quan tâm thực hiện./.

***Nơi nhận*:**
- Như kính gửi;
-Trang VPĐT Trung tâm;
- Lưu: VT, TCHC, pthuy.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

SỞ Y TẾ TỈNH AN GIANG
TRUNG TÂM Y TẾ KIÊN HẢI

Nguyễn Văn Cẩn

UBND TỈNH AN GIANG **SỞ Y TẾ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 524 /SYT-CNTTTT	*An Giang, ngày 29 tháng 7 năm 2025*

V/v thông báo tình hình hoạt động tấn công mạng, gián điệp mạng tại Việt Nam thời gian qua

Kính gửi: Các cơ quan, đơn vị thuộc, trực thuộc Sở Y tế

Thực hiện Công văn số 230/UBND-KGVX ngày 28/7/2025 của UBND tỉnh An Giang về việc thông báo tình hình hoạt động tấn công mạng, gián điệp mạng tại Việt Nam thời gian qua *(đính kèm);*

Sở Y tế triển khai Công văn số 230/UBND-KGVX đến các cơ quan, đơn vị thuộc, trực thuộc biết, thực hiện./.

Nơi nhận:
- Như trên;
- GĐ và các PGĐ SYT (để b/c);
- Trang Văn phòng điện tử SYT;
- Lưu: VT, CNTTTT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ Y TẾ
TỈNH AN GIANG

Nguyễn Thị Bích Hạnh

ỦY BAN NHÂN DÂN TỈNH AN GIANG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 230 /UBND-KGVX	*An Giang, ngày 28 tháng 7 năm 2025*

V/v thông báo tình hình hoạt động tấn công mạng, gián điệp mạng tại Việt Nam thời gian qua

Kính gửi:
- Các Sở, ban, ngành tỉnh;
- Ủy ban nhân dân xã, phường, đặc khu;
- Các tổ chức, doanh nghiệp nhà nước trên địa bàn tỉnh.

Thời gian qua, các nhóm tin tặc, gián điệp mạng với sự hậu thuẫn của chính phủ các nước gia tăng hoạt động, thực hiện các chiến dịch tấn công mạng nhằm vào hệ thống mạng, hạ tầng quan trọng để phá hoại, đánh cắp thông tin, dữ liệu. Tại Việt Nam, tình hình an ninh mạng tiếp tục diễn biến phức tạp, tiềm ẩn nguy cơ mất an ninh mạng, an toàn thông tin, lộ, mất bí mật nhà nước (BMNN) trên không gian mạng. Hoạt động tấn công, gián điệp mạng không chỉ đe dọa xâm phạm an ninh cơ sở hạ tầng trọng yếu, lộ, mất bí mật nhà nước, đồng thời còn gây thiệt hại nặng nề về tài chính, danh tiếng, độ tin cậy của cơ quan, tổ chức, doanh nghiệp bị tấn công, cụ thể:

1. Tình hình hoạt động tấn công mạng, gián điệp mạng

Trước thực trạng đầu tư, xây dựng hệ thống thông tin tại một số cơ quan, đơn vị chưa đồng bộ, được xây dựng từ lâu, theo công nghệ cũ, tồn tại nhiều điểm yếu, lỗ hổng bảo mật, cùng với đó nhận thức và ý thức chấp hành, thực hiện các quy định bảo đảm an ninh mạng, bảo vệ BMNN của một bộ phận cán bộ, công chức chưa thực sự nghiêm, các nhóm tin tặc , cơ quan đặc biệt nước ngoài đã triệt để lợi dụng, tổ chức các chiến dịch tấn công gián điệp mạng nguy hiểm, thường trực nhằm vào các cơ quan Trung ương, nhiều tỉnh, thành có vị trí quan trọng, chiến lược về kinh tế, quốc phòng, an ninh cũng như hạ tầng trọng yếu về năng lượng, giao thông, hàng không, cảng biên...

Hoạt động của các nhóm tin tặc hết sức tinh vi, sử dụng các dòng mã độc nguy hiểm được thiết kế riêng cho từng mục tiêu, ứng dụng trí tuệ nhân tạo tấn công, chiếm quyền điều khiển hệ thống thông tin của chính quyền các cấp, các cơ quan, đơn vị khối kinh tế tư nhân làm bàn đạp, tấn công leo thang các hệ thống thông tin trọng yếu của Đảng, Nhà nước, tự động đánh cắp gửi tài liệu ra bên ngoài ngay cả cách ly về mặt vật lý với mạng Internet như: Hệ thống phục

vụ hoạt động hành chính công, Dịch vụ công, một cửa..., hệ thống thư điện tử công vụ, hệ thống Quản lý văn bản và Điều hành phục vụ hoạt động quản lý, điều hành tác nghiệp... từ đó, các đối tượng tin tặc đã kiểm soát, thu thập nhiều tài liệu nội bộ, quan trọng về hoạt động chỉ đạo, điều hành chính quyền các cấp; việc xây dựng, triển khai các đề án, dự án phát triển kinh tế - xã hội, công tác quốc phòng - an ninh; kết quả thanh tra, kiểm tra xử lý các vụ việc nóng, phức tạp, kéo dài tại các địa phương.

2. Về phương thức, thủ đoạn tấn công mạng, gián điệp mạng

Qua phân tích, các nhóm tin tặc, gián điệp mạng nước ngoài sử dụng nhiều phương thức, thủ đoạn mới vô cùng tinh vi, nguy hiểm nhằm tấn công có chủ đích vào các hệ thống của các cơ quan trọng yếu để kiểm soát, phát tán mã độc và chiếm đoạt thông tin, tài liệu như:

(1) Tấn công phi kỹ thuật, nhất là tấn công lừa đảo (Phishing) là phương thức tấn công mạng phổ biến, trong đó người dùng bị lừa đảo, dẫn dụ mở đường dẫn hoặc tập tin độc hại trên các nền tảng trực tuyến, thư điện tử (Email, Zimbra và Roundcube) thông qua tin nhắn mạo danh tài liệu hội nghị, đề nghị cộng tác, mời tham dự sự kiện, tuyển dụng, mời quảng cáo... để phát tán mã độc hay đánh cắp thông tin nhạy cảm của nạn nhân trong mục tiêu;

(2) Thiết kế các mã độc mới, dùng riêng nhằm vào các cơ quan trọng yếu; sử dụng các ứng dụng thông thường để kích hoạt, giải mã và thực thi các tệp tin chứa đoạn mã độc hại; sử dụng cơ chế tái lây nhiễm mỗi khi hệ thống khởi động lại. Do vậy, mặc dù hệ thống đã được triển khai phần mềm diệt virus và giải pháp bảo vệ, giám sát an ninh mạng của các đơn vị nhưng vẫn không thể phát hiện được. Các mã độc này chỉ được phát hiện qua biện pháp kỹ thuật chuyên biệt và được phân tích kỹ phương thức hoạt động thông qua triển khai các biện pháp đấu tranh của Bộ Công an;

(3) Khai thác lỗ hổng bảo mật Zero-day trên các ứng dụng, phần mềm văn phòng phổ biến (như Microsoft office, PDF reader) để đính kèm mã độc vào các tập tin văn bản, lây nhiễm vào máy tính, thiết bị khi người dùng mở tập tin;

(4) Tấn công chuỗi cung ứng thông qua lợi dụng dịch vụ lưu trữ đám mây (Google Drive, OneDrive), kho lưu trữ phần mềm (PyPI), nền tảng quản lý mã nguồn (Github, Bitbucket) hay giả mạo các phần mềm hợp pháp (bản cập nhật Java, 7-zip) để lây nhiễm mã độc vào hệ thống mạng của mục tiêu;

(5) Sử dụng đồng thời nhiều dòng mã độc khác nhau để tấn công, xâm nhập, khống chế hệ thống mạng. Đặc biệt, các dòng mã độc gián điệp này có cơ chế thông minh, ứng dụng trí tuệ nhân tạo (AI) để khai thác lỗ hổng hệ thống, xâm nhập sâu, lan rộng, đồng thời ẩn mình qua chính các máy chủ phòng chống

virus, kết hợp với nhiều kịch bản tấn công mà nếu không được phát hiện, bóc gỡ triệt để, chúng sẽ lại tái kiểm soát, khống chế toàn bộ mạng;

(6) Sử dụng mã độc tống tiền (Ransomware) nhằm vào các mục tiêu cơ sở hạ tầng quan trọng như y tế, tài chính, giao thông vận tải và tiện ích công cộng;

(7) Tấn công khai thác, lỗ hổng bảo mật trên các máy chủ có quyền quản trị trong hệ thống máy chủ quản trị miền, máy chủ phòng chống mã độc tập trung và lợi dụng chính những thiết bị bảo mật này để triển khai các kịch bản tấn công xuống máy trạm nhằm hạn chế để lại dấu vết và duy trì tình trạng kiểm soát;

(8) Sử dụng nhiều máy chủ, máy trạm trong hệ thống làm các điểm trung chuyển tài liệu và kho mã độc trung gian, từ đó kết nối đến mạng lưới máy chủ điều khiển rộng lớn, với nhiều máy chủ dự phòng để duy trì tình trạng kiểm soát hệ thống.

3. Nguyên nhân dẫn đến tình trạng mất an ninh mạng, an toàn thông tin, lộ, mất BMNN trên không gian mạng, chủ yếu là do:

(1) Các cơ quan, đơn vị, tổ chức, doanh nghiệp, địa phương chưa triển khai đầy đủ các biện pháp bảo vệ an ninh mạng, bảo đảm an toàn thông tin theo quy định, gây khó khăn cho công tác phát hiện, ngăn chặn, xử lý hoạt động tấn công mạng, gián điệp mạng trên các hệ thống thông tin thuộc phạm vi quản lý;

(2) Nhận thức, ý thức của một bộ phận không nhỏ lãnh đạo, cán bộ, công chức, viên chức tại các sở, ban, ngành, địa phương, tổ chức, doanh nghiệp còn chủ quan, mất cảnh giác, chưa chấp hành đúng các quy định về bảo đảm an ninh mạng, bảo vệ BMNN, bảo vệ dữ liệu cá nhân; trách nhiệm của người đứng đầu chưa được thể hiện rõ, dẫn đến nhiều chính sách của Đảng, Nhà nước, quy định của pháp luật không được quán triệt thực hiện nghiêm túc;

(3) Còn tình trạng cán bộ, công chức sử dụng máy tính không đúng mục đích, sử dụng máy tính kết nối Internet để soạn thảo, lưu trữ tài liệu BMNN, dùng chung thiết bị lưu trữ ngoại vi (USB, ổ cứng di động...) giữa máy tính kết nối Internet và máy tính độc lập lưu trữ, soạn thảo tài liệu BMNN; sử dụng thư điện tử công vụ, hệ thống quản lý văn bản và điều hành, dịch vụ nhắn tin đa phương tiện (OTT) trên môi trường mạng Internet để gửi/nhận văn bản, tài liệu BMNN; sử dụng các tài khoản công vụ với mật khẩu mặc định, mật khẩu yếu, lưu thông tin tài khoản/mật khẩu trên trình duyệt;

(4) Bộ phận chuyên trách về công nghệ thông tin chưa trang bị đầy đủ kiến thức về an ninh mạng, chưa nhận thức được mức độ nghiêm trọng của việc hệ thống bị tấn công, xâm nhập, lây nhiễm mã độc; không quyết liệt thực hiện

việc rà soát, khắc phục, bóc gỡ mã độc khi nhận được thông báo của cơ quan chức năng;

(5) Công tác xử lý cán bộ, công chức tại các cơ quan, đơn vị trong vi phạm các quy định về đảm bảo an ninh mạng, an toàn thông tin, để lộ tài liệu BMNN thời gian qua còn nhiều hạn chế, thiếu tính răn đe, dẫn đến tình trạng vi phạm tái diễn mà chưa có chuyển biến, còn tình trạng chủ quan, thiếu nghiêm túc trong thực hiện quy định của pháp luật.

Căn cứ Thông báo số 55/TB-BCA-A05 ngày 09/6/2025 của Bộ Công an về tình hình hoạt động tấn công mạng, gián điệp mạng tại Việt Nam thời gian qua, để kịp thời phát hiện, ngăn chặn, xử lý tình trạng mất an ninh mạng, an toàn thông tin, lộ, mất BMNN trên các hệ thống thông tin thuộc phạm vi quản lý; Chủ tịch Ủy ban nhân dân tỉnh yêu cầu các Sở, ban, ngành cấp tỉnh, Ủy ban nhân dân các xã, phường, đặc khu, các tổ chức, doanh nghiệp nhà nước trên địa bàn tỉnh thực hiện một số nội dung sau:

1. Tiếp tục quán triệt và thực hiện nghiêm túc các quy định của Đảng, Nhà nước, thông báo, hướng dẫn của Bộ Công an về công tác bảo đảm an ninh mạng, bảo vệ BMNN, bảo vệ dữ liệu cá nhân như: Luật An ninh mạng, Luật Bảo vệ bí mật nhà nước, Nghị định số 13/2023/NĐ-CP, ngày 17/4/2023 của Chính phủ quy định về bảo vệ dữ liệu cá nhân và các văn bản hướng dẫn thi hành; Chỉ thị số 01/CT-TTg, ngày 18/02/2021 của Thủ tướng Chính phủ về tăng cường công tác bảo vệ an ninh mạng trong tình hình hiện nay... Xây dựng và hoàn thiện quy định quản lý, sử dụng và bảo đảm an ninh mạng máy tính nội bộ, mạng máy tính có kết nối Internet; quy trình quản lý, cấp phát, thu hồi, sử dụng tài khoản công vụ, tài khoản truy cập hệ thống thông tin phục vụ hành chính công, Dịch vụ công, một cửa; phương án bảo đảm an ninh mạng; phương án ứng phó, khắc phục sự cố an ninh mạng các hệ thống thông tin thuộc phạm vi quản lý theo quy định.

2. Tổ chức rà soát, khắc phục sơ hở, thiếu sót trong công tác quản lý, quản trị, vận hành hệ thống mạng máy tính tại cơ quan, đơn vị. Định kỳ, đột xuất tiến hành kiểm tra an ninh mạng, tăng cường giám sát an ninh mạng, kiểm soát truy cập mạng để kịp thời phát hiện các nguy cơ mất an ninh mạng, an toàn thông tin; rà soát gỡ bỏ virus, mã độc trên máy tính, hệ thống mạng máy tính.

3. Đầu tư cơ sở vật chất, trang thiết bị kỹ thuật nhằm bảo đảm an ninh mạng, an toàn thông tin. Rà soát, đánh giá lại toàn bộ hệ thống thông tin tại cơ quan, đơn vị, thay thế các mô hình mạng, giải pháp đảm bảo an ninh mạng đã lỗi thời bằng các giải pháp, thiết bị mới; trang bị thêm các giải pháp phòng, chống virus, mã độc, quản lý thiết bị đầu cuối tập trung; hệ thống giám sát, phát hiện, cảnh báo hoạt động tấn công mạng (SIEM/SOC); không mua sắm mới thiết bị

có nguồn gốc, xuất xứ từ một số quốc gia, hãng công nghệ đã bị cảnh báo tồn tại lỗ hổng bảo mật, có nguy cơ mất an ninh mạng, an toàn thông tin; đẩy mạnh nghiên cứu ứng dụng trí tuệ nhân tạo (AI) phục vụ triển khai có hiệu quả các biện pháp kỹ thuật nhằm giám sát, phát hiện và vô hiệu hóa hoạt động tấn công mạng, gián điệp mạng.

4. Chú trọng tuyên truyền, đào tạo, tập huấn, nâng cao nhận thức của người dùng, cán bộ, công chức về bảo đảm an ninh mạng, bảo vệ BMNN, bảo vệ dữ liệu cá nhân, đảm bảo an toàn trong quá trình quản lý, sử dụng máy tính, tài khoản công vụ truy cập các hệ thống quản lý, điều hành tác nghiệp, hệ thống hành chính công, Dịch vụ công một cửa; tập huấn chuyên sâu về an ninh mạng cho bộ phận chuyên trách về công nghệ thông tin, quản trị hệ thống.

5. Phát huy vai trò, trách nhiệm của người đứng đầu cơ quan, đơn vị đối với công tác bảo đảm an ninh mạng, an toàn thông tin, bảo vệ BMNN; xử lý nghiêm các tập thể, cá nhân vi phạm các quy định, quy chế để xảy ra tình trạng mất an ninh mạng, an toàn thông tin, lộ, mất dữ liệu nội bộ, tài liệu BMNN.

Chủ tịch Ủy ban nhân dân tỉnh yêu cầu các Sở, ban, ngành, đơn vị tỉnh và các địa phương tổ chức triển khai thực hiện theo tinh thần chỉ đạo tại Công văn này./.

Nơi nhận:
- Như trên;
- CT và các PCT UBND tỉnh;
- Công an tỉnh;
- LĐVP;
- Phòng KGVX;
- Lưu: VT, ntgiang.

CHỦ TỊCH

Hồ Văn Mừng