

BỘ CÔNG AN
CÔNG AN TỈNH ĐỒNG NAI

Số 2395/CAT-PA05

V/v cảnh báo mã độc Valley RAT và tăng
cường đảm bảo an toàn thông tin mạng

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

Đồng Nai, ngày 03 tháng 11 năm 2025

Kính gửi:

- Các sở, ban, ngành của tỉnh;
- UBND các phường, xã.

Qua công tác phối hợp giám sát đảm bảo an ninh, an toàn thông tin mạng cho các hệ thống thông tin của tỉnh, Công an tỉnh đã ghi nhận chiến dịch tấn công mạng có chủ đích thông qua việc phát tán các tệp tin độc hại giả mạo văn bản hành chính của cơ quan nhà nước¹. Qua phân tích, phát hiện các tệp tin này chứa mã độc Valley RAT - một loại *Remote Access Trojan (RAT)* có khả năng chiếm quyền điều khiển hệ thống, tải thêm plugin độc hại và đánh cắp dữ liệu. Mã độc này liên kết với máy chủ điều khiển (C2) có địa chỉ 27.124.9.13. Khi người dùng mở tệp tin, hệ thống sẽ bị chiếm quyền điều khiển, dẫn đến nguy cơ rò rỉ dữ liệu, mất an ninh, an toàn thông tin.

Để chủ động phòng ngừa và hạn chế thiệt hại do mã độc gây ra, Công an tỉnh Đồng Nai đề nghị các cơ quan, đơn vị, địa phương khẩn trương triển khai các nội dung sau:

1. Tiếp tục triển khai cài đặt phần mềm diệt virus EDR theo Công văn số 59/SKHCN-CĐS ngày 08/7/2025 của Sở Khoa học và Công nghệ đối với toàn bộ máy tính Các sở, ban, ngành; UBND các phường, xã trên địa bàn toàn tỉnh Đồng Nai.

2. Xây dựng phương án ứng cứu sự cố an toàn thông tin mạng trên cơ sở Kế hoạch số 79/KH-UBND ngày 05/9/2025 của UBND tỉnh Đồng Nai và gửi kết quả về Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao).

3. Khẩn trương xây dựng hồ sơ cấp độ an toàn hệ thống thông tin, trong đó các đơn vị cần nghiên cứu kỹ các văn bản hướng dẫn như Nghị định 85/2016/CP ngày 01/7/2016 của Chính phủ và Thông tư số 12/2022/TT-BTTTT

¹ DỰ THẢO NGHỊ QUYẾT ĐẠI HỘI.exe, BÁO CÁO TÀI CHÍNH2.exe, CÔNG VĂN HÒA TỐC CỦA CHÍNH PHỦ.exe, HỒ TRỢ KÊ KHAI THUẾ.exe, BIÊN BẢN BÁO CÁO QUÝ III.exe

ngày 12/8/2022 của Bộ Thông tin và Truyền thông, đồng thời phối hợp Công an tỉnh (*đơn vị chuyên trách đảm bảo an toàn thông tin mạng của tỉnh Đồng Nai*) trước khi đề nghị thẩm định và phê duyệt cấp độ.

4. Khi xảy ra sự cố (bị nhiễm mã độc, mất an toàn thông tin...) cần khẩn trương cô lập thiết bị, ngắt kết nối Internet, ghi nhận lại hoạt động bất thường và báo ngay cho cán bộ phụ trách an toàn thông tin hoặc Bộ phận thường trực của Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Đồng Nai, địa chỉ: Số 1374 đường Phạm Văn Thuận, phường Tam Hiệp, tỉnh Đồng Nai; số điện thoại: 02513.685.134; địa chỉ thư điện tử: ucsc@dongnai.gov.vn để được hỗ trợ, xử lý.

Công an tỉnh Đồng Nai đề nghị lãnh đạo các cơ quan, đơn vị, địa phương quan tâm, chỉ đạo thực hiện nghiêm túc các nội dung trên. Trong quá trình triển khai, nếu có khó khăn, vướng mắc, đề nghị liên hệ Công an tỉnh Đồng Nai (*qua đồng chí Thiếu tá Nguyễn Chí Hiếu – Phó Đội trưởng, Phòng an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, số điện thoại 0394 443 637*) để được phối hợp thực hiện./.

Nơi nhận:

- Như trên;
- Lưu: VT, PA05.



Đại tá Nguyễn Phương Đăng