UBND TỈNH HÀ TĨNH
SỞ TƯ PHÁP

Số: 3587/STP-VP

V/v tăng cường các biện pháp kỹ thuật, nâng cao ý thức bảo mật để phòng chống mã độc và khắc phục lỗ hổng an ninh mạng

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

Hà Tĩnh, ngày 30 tháng 11 năm 2025

Kính gửi: Các Phòng, Trung tâm thuộc Sở

Thực hiện các Văn bản của Công an tỉnh: số 3935/CAT-ANM ngày 09/11/2025 về việc cảnh báo mã độc nguy hiểm Valley RAT giả dạng tập tin văn bản, số 3918/CAT-ANM ngày 03/11/2025 về việc thông báo lỗ hổng bảo mật nghiêm trọng tháng 10/2025, Sở Tư pháp yêu cầu các Phòng, Trung tâm thuộc Sở nghiêm túc triển khai các nội dung sau:

1. Triển khai khẩn cấp Phòng chống Mã độc Valley RAT (Valley RAT)

Các đơn vị triển khai rà soát hệ thống và thực hiện nghiêm các biện pháp sau để đối phó với mã độc Valley RAT, loại mã độc đa giai đoạn, có khả năng giám sát và kiểm soát hệ thống:

- Rà soát toàn bộ máy tính cá nhân và hệ thống để tìm kiếm các tập tin nghi ngờ (ví dụ: DỰ THẢO NGHỊ QUYẾT ĐẠI HỘI.exe, BÁO CÁO TÀI CHÍNH2.exe, CÔNG VĂN HỎA TỐC CỦA CHÍNH PHỦ.exe, v.v.).

- Khi phát hiện sự cố (máy tính bị nhiễm), phải cách ly máy tính bị nhiễm mã độc ngay lập tức bằng cách ngắt kết nối Internet/mạng LAN.

- Sử dụng các phần mềm bảo mật có khả năng phát hiện và diệt mã độc (như Windows Defender bản cập nhật mới nhất, Avast bản free, AVG bản free, Bitdefender bản free) để rà quét toàn bộ hệ thống.

- Bộ phận CNTT khẩn trương kiểm tra, thiết lập chặn truy cập đến địa chỉ IP độc hại: 27.124.9.13 trên thiết bị tường lửa (Firewall) hoặc thiết bị chặn IP tương đương.

- Tuyệt đối không mở các tập tin đính kèm có đuôi .exe hoặc các tệp tin không rõ nguồn gốc, đặc biệt là các tệp tin nhận được qua email lừa đảo (phishing).

2. Khắc phục lỗ hổng bảo mật nghiêm trọng và nâng cao nhận thức về an ninh mạng

2.1. Các đơn vị rà soát và thực hiện cập nhật, vá lỗi ngay đối với các lỗ hổng nghiêm trọng đã được Công an tỉnh cảnh báo, trong đó:

- Yêu cầu toàn bộ công chức, viên chức, người lao động gỡ bỏ phiên bản 7-Zip cũ (từ phiên bản 21.02 đến trước phiên bản 25.00) và cài đặt phiên bản mới

nhất (25.00 trở lên) từ trang chủ nhà phát hành để khắc phục lỗ hổng CVE-2025-11001 (mức độ rất nghiêm trọng).

- Tuyệt đối không giải nén các tệp tin không rõ nguồn gốc nhận từ email hoặc các nguồn không tin cậy.

- Rà soát và cài đặt các bản vá bảo mật mới nhất của Microsoft thông qua dịch vụ Windows Update để khắc phục lỗ hổng leo thang đặc quyền CVE-2025-59230 (Windows Remote Access Connection Manager).

- Thực hiện sao lưu dữ liệu quan trọng của hệ thống và người dùng một cách định kỳ, đảm bảo lưu trữ các bản sao lưu tách biệt với hệ thống chính (offline) để có thể khôi phục khi xảy ra sự cố.

- Tăng cường giám sát, theo dõi nhật ký (log) hệ thống để sớm phát hiện các dấu hiệu tấn công, xâm nhập bất thường.

2.2. Nâng cao nhận thức cho công chức, viên chức về các nguy cơ an ninh mạng, tuyệt đối cẩn trọng với các email, tin nhắn lạ, các tệp đính kèm và đường dẫn đáng ngờ.

Đề nghị các Phòng, Trung tâm nghiêm túc, triển khai thực hiện có hiệu quả các nội dung trên. Khi phát hiện dấu hiệu mất an ninh mạng, an toàn thông tin (mã độc, tấn công mạng, xâm nhập) các Phòng, Trung tâm thuộc Sở phải cách ly máy tính ngay lập tức và khẩn trương báo cáo về Văn phòng Sở là đầu mối tiếp nhận ứng cứu sự cố của Sở để phối hợp với Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh kịp thời xử lý./.

Nơi nhận:
- Như trên;
- Lãnh đạo Sở;
- Lưu: VT, VP.

TL. GIÁM ĐỐC
CHÁNH VĂN PHÒNG

CỘNG HÒA XHCN VIỆT NAM
SỞ TƯ PHÁP
TỈNH HÀ TĨNH

Trần Thị Kiều Oanh