BỘ CÔNG AN
CÔNG AN TỈNH HÀ TĨNH

Số: 5038/CAT-KTNV&NT

V/v cảnh báo mã độc nguy hiểm lây nhiễm qua lỗ hổng bảo mật

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

Hà Tĩnh, ngày09 tháng 11 năm 2026

Kính gửi:
- Các Ban, Cơ quan, Đảng ủy trực thuộc Tỉnh ủy;
- Văn phòng: Tỉnh ủy, HĐND tỉnh, UBND tỉnh;
- Mặt trận Tổ quốc, Đoàn thể chính trị - xã hội cấp tỉnh;
- Các sở, ban, ngành, đơn vị sự nghiệp trên địa bàn tỉnh;
- Đảng uỷ, HĐND, UBND các xã, phường.

Thực hiện công tác kiểm tra an ninh an toàn thông tin đối với các hệ thống, thiết bị điện tử, thông tin liên lạc của các cơ quan, đơn vị, tổ chức trên địa bàn, Công an tỉnh Hà Tĩnh phát hiện và cảnh báo về việc lây nhiễm, tán phát các loại mã độc nguy hiểm qua lỗ hổng bảo mật đến các máy tính, thiết bị điện tử có chưa BMNN, như sau:

1. Thông tin cảnh báo mã độc Backdoor.bot (WinAlert.exe, Commgr.exe, winsysapp.exe).

Đây là loại mã độc lây lan mạnh mẽ thông qua nhiều hình thức đặc biệt là các lỗ hổng bảo mật nghiêm trọng từ những bản Window cũ chưa được cập nhật bản vá. Mã độc có thể khóa các quyền của tài khoản Administrator (regedit, taskmanage, cmd…), tắt chức năng hiển thị các file ẩn trên máy, chèn một số chương trình vào máy để mở một số cổng quan trọng cho việc điều khiển từ xã từ đó thu thập, đánh cắp thông tin, dữ liệu nhạy cảm của cơ quan, đơn vị, đồng thời tạo tiền đề mở cổng hậu cho các cuộc tấn công mã hóa dữ liệu tống tiền (ransomware) nguy hiểm.

2. Dấu hiệu nhiễm mã độc:

- Dấu hiệu về hiệu năng

+ CPU hoặc RAM tăng bất thường khi không chạy ứng dụng.

+ Có tiến trình lạ chạy nền.

+ Máy tính tự động truy cập Internet dù không có thao tác.

+ Máy chậm, treo hoặc xuất hiện các kết nối mạng bất thường.

- Dấu hiệu về hệ thống

+ Xuất hiện tài khoản Windows không rõ nguồn gốc.

+ Có dịch vụ Windows mới được tạo.

+ Task Scheduler xuất hiện tác vụ lạ.

+ Windows Defender bị vô hiệu hóa hoặc thay đổi cấu hình.

+ Có chương trình tự khởi động cùng Windows mà bạn không cài đặt.

3. Nguồn lây

- Phần mềm không rõ nguồn gốc: Crack, keygen, phần mềm kích hoạt Windows hoặc Office giả mạo.

- Tệp đính kèm email: Tệp EXE, ZIP, RAR hoặc tài liệu chứa mã độc.

- USB: Tệp thực thi giả mạo hoặc mã độc tự sao chép.

- Lỗ hổng Windows: Khai thác những lỗ hổng chưa được vá.

- Mã độc khác: Một Trojan khác tải Backdoor.Bot về và cài đặt.

4. Biện pháp khắc phục và xử lý

Do loại mã độc này có tốc độ lây nhiễm nhanh, khó phát hiện đối với các máy tính không được cập nhật cơ sở dữ liệu của phần mềm bảo mật, Công an tỉnh đề nghị các đơn vị, địa phương chỉ đạo triển khai ngay các biện pháp sau:

- Sau khi phát hiện các dấu hiệu nhiễm mã độc phải cách ly máy tính nghi nhiễm khỏi hệ thống LAN, WAN nội bộ, Internet.

- Tiến hành đổi thông tin bảo mật tại các tài khoản đã sử dụng máy tính để đăng nhập, xóa dữ liệu (lịch sử, mật khẩu đã lưu, cookie, cache,…) của các trình duyệt Web đang sử dụng.

- Sử dụng các phần mềm diệt mã độc offline như Microsoft Defender Offline, Kaspersky Virus Removal Tool,… để tiến hành rà quét và xóa bỏ các tập tin lây nhiễm.

- Luôn bật và duy trì hoạt động của phần mềm diệt virus như Smart IR, Kapersky,… trên máy tính công tác.

- Sử dụng máy tính có hệ điều hành, phần mềm có bản quyền.

- Không tự ý cài đặt các phần mềm, tải các file lạ trôi nổi trên Internet khi chưa được phân tích nguy cơ tiềm ẩn

Công an tỉnh thông báo và đề nghị các cơ quan, đơn vị thực hiện nghiêm túc, đồng thời phổ biến, quán triệt đến các đơn vị trực thuộc để thực hiện./.

Nơi nhận:
- Như trên;
- Đ/c Giám đốc (để báo cáo);
- Lưu: VT, KTNV&NT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CÔNG HOÀ X.H.C.N VIỆT NAM
CÔNG AN TỈNH HÀ TĨNH

Thượng tá Nguyễn Quốc Hùng