

Số: 2087 /STP-VP

Hà Tĩnh, ngày 11 tháng 8 năm 2026

V/v thông báo lỗ hổng bảo mật
nghiêm trọng tháng 7/2026

Kính gửi: Các Phòng, Trung tâm thuộc Sở

Thực hiện Công văn số 3341/CAT-ANM ngày 06/8/2026 của Công an tỉnh Hà Tĩnh về việc thông báo lỗ hổng bảo mật nghiêm trọng tháng 7/2026, theo đó trên không gian mạng xuất hiện nhiều chiến dịch tấn công mạng tinh vi và các lỗ hổng nghiêm trọng trên các phần mềm, ứng dụng phổ biến, tiềm ẩn nguy cơ bị chiếm quyền điều khiển hệ thống, đánh cắp và mã hóa dữ liệu đòi tiền chuộc (ransomware); để chủ động phòng ngừa, bảo đảm an toàn thông tin trong hoạt động của Sở, Sở Tư pháp yêu cầu Trưởng các phòng, Trung tâm thuộc Sở khẩn trương thực hiện các nội dung sau:

1. Quán triệt, phổ biến đến toàn thể công chức, viên chức, người lao động thuộc đơn vị mình quản lý các nguy cơ tấn công mạng và lỗ hổng bảo mật nghiêm trọng đã được Công an tỉnh cảnh báo, cùng biện pháp phòng ngừa tương ứng, cụ thể:

1.1. Lọt lộ bí mật nội bộ khi dùng các công cụ AI tạo sinh công cộng (ChatGPT, Claude, Copilot, DeepSeek...)

Mức độ: Nghiêm trọng

Mô tả: Khi công chức, viên chức nhập trực tiếp tài liệu chưa công bố, hợp đồng, báo cáo, mã nguồn hoặc thông tin cá nhân của công dân vào các ứng dụng AI công cộng để nhờ tóm tắt, chỉnh sửa, soạn thảo, toàn bộ dữ liệu có thể bị lưu trên máy chủ của đơn vị cung cấp dịch vụ, sau đó có thể bị dùng để huấn luyện AI hoặc vô tình rò rỉ ra ngoài khi hệ thống AI gặp sự cố bảo mật.

Biện pháp: Tuyệt đối không nhập thông tin bí mật nhà nước, dữ liệu cá nhân của công dân, mã nguồn, thông tin nội bộ chưa công khai vào các công cụ AI công cộng trên Internet.

1.2. Website/tiện ích mở rộng (extension) giả mạo AI (ChatGPT, DeepSeek, Claude...) để phát tán mã độc

Mức độ: Nghiêm trọng

Mô tả: Tin tặc lợi dụng trào lưu sử dụng công cụ AI để tạo ra trang web, phần mềm hoặc tiện ích trình duyệt giả mạo dưới các tên gọi quen thuộc. Khi người dùng tải về, cài đặt, phần mềm sẽ bí mật chạy kịch bản độc hại nhằm chiếm quyền điều khiển máy tính, lấy cắp mật khẩu lưu trên trình duyệt, thông tin thẻ tín dụng và tài khoản ngân hàng.

Biện pháp: Chỉ cài đặt ứng dụng, tiện ích từ nguồn chính thức (Chrome Web Store, Microsoft Store); tuyệt đối không tải phần mềm từ link chia sẻ trên mạng xã hội hoặc tệp đính kèm email.

1.3. Lỗ hổng “backdoor” trong công cụ Claude Code (phiên bản 2.1.91 - 2.1.196)

Mức độ: Nghiêm trọng

Mô tả: Cơ quan Cơ sở dữ liệu lỗ hổng quốc gia (NVDB) đã phát hiện lỗ hổng dạng “cửa sau” (backdoor) trong các phiên bản 2.1.91 đến 2.1.196 của công cụ hỗ trợ lập trình Claude Code, cho phép công cụ tự động truyền thông tin nhạy cảm của người dùng (vị trí địa lý, mã định danh cá nhân...) về máy chủ từ xa mà không có sự đồng ý hay thông báo cho người sử dụng.

Biện pháp: Đơn vị nào có công chức, viên chức sử dụng công cụ hỗ trợ lập trình Claude Code cần rà soát ngay phiên bản đang cài đặt; nếu thuộc khoảng 2.1.91-2.1.196 phải gỡ bỏ hoặc cập nhật lên phiên bản mới nhất ngay.

1.4. Virus đa hình Virus.Win32.Virut.ce/Virus.Win64.Moiva.a (lây nhiễm toàn bộ tệp .exe, .scr, mở backdoor)

Mức độ: Đặc biệt nghiêm trọng

Mô tả: Là dòng virus loại “File Infector” nguy hiểm, tự động chèn mã độc vào mọi tệp thực thi trên máy (kể cả tệp lỗi hệ điều hành), có tính “đa hình” (tự thay đổi cấu trúc mã sau mỗi lần lây nhiễm) khiến phần mềm diệt virus khó nhận diện; mở “cửa sau” kết nối máy chủ điều khiển (C&C) để tin tặc chiếm quyền kiểm soát, đánh cắp thông tin, biến máy thành công cụ tấn công khác (Botnet); lây lan rất nhanh qua USB, ổ cứng di động, thư mục chia sẻ mạng nội bộ.

Biện pháp: Khi nghi nhiễm phải ngắt kết nối Internet, rút thiết bị lưu trữ ngoài; không tự diệt virus bằng phần mềm thông thường; sao lưu dữ liệu tài liệu (docx, pdf, xlsx - không sao lưu file .exe), sau đó cài lại hệ điều hành; liên hệ đầu mối cài Smart IR để được cấp lại Key.

1.5. Macro-virus qua file Excel (Virus.MSExcel.Laroux), lây lan qua Zalo

Mức độ: Nghiêm trọng

Mô tả: Là loại macro-virus lây lan qua file Excel, phát tán mạnh qua ứng dụng Zalo. Khi người dùng mở file và bấm “cho phép Macros” (Enable Macros), virus sẽ lây nhiễm vào hệ thống, có khả năng đánh cắp thông tin nhạy cảm và là tiền đề cho các cuộc tấn công mã hóa dữ liệu đòi tiền chuộc (ransomware).

Biện pháp: Tuyệt đối không bấm “cho phép Macros/Enable Content” với file nhận từ nguồn không tin cậy; luôn bật phần mềm diệt virus Smart IR.

1.6. Virus lây nhiễm qua phần mềm AutoCAD

Mức độ: Nghiêm trọng

Mô tả: Virus lây nhiễm vào môi trường làm việc của phần mềm AutoCAD; khi người dùng mở một tệp bản vẽ bất kỳ, mã độc sẽ được kích hoạt và có khả năng đánh cắp, phá hoại các bản vẽ thiết kế, dữ liệu quy hoạch, dự án quan trọng.

Biện pháp: Không rõ nguồn gốc, báo cáo ngay cho bộ phận công nghệ thông tin khi phần mềm AutoCAD có các biểu hiện bất thường và luôn bật phần mềm diệt virus Smart IR.

1.7. Mã độc trung gian Trojan-Dropper.VBS.Agent.bp (ẩn trong file .zip/.rar, kịch bản .vbs/.js qua email)

Mức độ: Nghiêm trọng

Mô tả: Mã độc không trực tiếp gây hại mà đóng vai trò công cụ trung gian, âm thầm tải và cài đặt các mã độc nguy hiểm khác vào hệ thống (phần mềm theo dõi bàn phím, đánh cắp thông tin cá nhân hoặc mã hóa dữ liệu đòi tiền chuộc); thường ẩn trong tệp tài liệu, tệp kịch bản hoặc tệp nén (.zip, .rar) gửi qua email, tin nhắn từ nguồn không xác định.

Biện pháp: Không mở tệp đính kèm đuôi lạ hoặc nén từ người gửi không rõ danh tính; kiểm tra kỹ tên, định dạng tệp trước khi mở.

1.8. File .exe không rõ nguồn gốc phát tán qua email, Zalo, Telegram, USB

Mức độ: Nghiêm trọng

Mô tả: Một số tệp thực thi (.exe) tại các đơn vị đã ghi nhận có hành vi nguy hiểm, tiềm ẩn rủi ro cao với hệ thống thông tin; khi bị vô tình thực thi, mã độc có thể được kích hoạt, cho phép kẻ tấn công xâm nhập hệ thống, tải thêm mã độc khác, duy trì quyền kiểm soát và là tiền đề cho các cuộc tấn công mã hóa dữ liệu tổng tiền (ransomware) trong tương lai.

Biện pháp: Không chạy file .exe nhận từ nguồn không rõ ràng; không tải phần mềm crack, keygen; luôn bật Smart IR.

2. Bảo đảm 100% máy tính công vụ được cài đặt, bật thường xuyên phần mềm diệt virus Smart IR; các đơn vị sự nghiệp thuộc Sở chưa cài đặt hoặc cần cập lại Key, liên hệ đầu mối VNPT (Đồng chí Đặng Quốc Sinh, số điện thoại 0975357960) để được hỗ trợ.

Đề nghị Thủ trưởng các Phòng, Trung tâm thuộc Sở chỉ đạo, tổ chức thực hiện kịp thời và có hiệu quả. Khi phát hiện dấu hiệu bất thường, mã độc hoặc bị tấn công, kịp thời báo cáo Văn phòng Sở để phối hợp xử lý; trường hợp cần thiết liên hệ Phòng An ninh mạng và Phòng chống tội phạm sử dụng Công nghệ cao - Công an tỉnh (SDT: 099.338.6777) để được hỗ trợ./.

Nơi nhận:

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

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**



Đinh Văn Hồng