BỘ CÔNG AN
**CÔNG AN TỈNH HÀ TĨNH**

Số: 634/CAT-ANM

V/v thông báo lỗ hổng bảo mật nghiêm trọng tháng 4/2026

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

*Hà Tĩnh, ngày 06 tháng 05 năm 2026*

Kính gửi:
- Các Ban Đảng, UBKT, Văn phòng Tỉnh ủy;
- Các Đảng ủy trực thuộc Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các sở, ban, ngành, đoàn thể cấp tỉnh;
- Các doanh nghiệp nhà nước trên địa bàn tỉnh;
- Đảng ủy, UBND cấp xã.

Tháng 4/2026 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. Đặc biệt hệ thống quản trị mã độc tập trung ghi nhận một số loại mã độc nguy hiểm đang lây nhiễm, ảnh hưởng trực tiếp đến các cơ quan, đơn vị trên địa bàn tỉnh. Các loại virus, mã độc này có thể bị đối tượng tấn công lợi dụng để chiếm quyền điều khiển hệ thống, đánh cắp và mã hóa dữ liệu đòi tiền chuộc (ransomware). Công an tỉnh thông báo thông tin và hướng dẫn các đơn vị giải pháp khắc phục như sau:

**1. Các nguy cơ tấn công mạng và lỗ hổng bảo mật nghiêm trọng**

**1.1.** Cảnh báo chiếm quyền Zalo qua "Mã QR bình chọn"

- Mức độ: Đặc biệt nghiêm trọng.

- Mô tả: Thủ đoạn "Bình chọn cuộc thi" đã nâng cấp. Thay vì chỉ gửi link đăng nhập, đối tượng hiện nay gửi Mã QR giả mạo là mã bình chọn hoặc mã nhận quà. Khi nạn nhân dùng Zalo quét mã này thực chất là đang thực hiện lệnh "Đăng nhập Zalo Web" trên thiết bị của kẻ tấn công. Ngay khi chiếm được quyền, đối tượng sử dụng công nghệ AI Deepfake để tạo ra các đoạn tin nhắn thoại hoặc hình ảnh cử động giống hệt chủ tài khoản để nhắn tin vay mượn tiền, khiến người thân trong danh bạ rất khó phân biệt thật giả. Hoặc đối tượng sẽ âm thầm thu thập dữ liệu tin nhắn, thông tin cá nhân nhạy cảm của người dùng.

- Ảnh hưởng: Tất cả người dùng Zalo, đặc biệt nguy hiểm với những người thường xuyên tham gia các hội nhóm cộng đồng, từ thiện, phụ huynh học sinh.

- Giải pháp khắc phục: (1) Tuyệt đối không quét các mã QR lạ được gửi qua tin nhắn để "Bình chọn" hay "Nhận quà". (2) Luôn kiểm tra mục "Cài đặt > Tài khoản và bảo mật > Lịch sử đăng nhập", nếu thấy có thiết bị "Zalo Web" lạ phải bấm "Đăng xuất" ngay lập tức. (3) Thiết lập mã khóa ứng dụng (PIN) để ngăn chặn việc truy cập trái phép từ xa.

**1.2.** Cảnh báo thủ đoạn thuê SIM "rác" để chiếm đoạt tài khoản từ số điện thoại cũ

- Mức độ: Rất nghiêm trọng.

- Mô tả: Đây là lỗ hổng trong quản lý thông tin cá nhân, các đối tượng thuê lại SIM số điện thoại cũ đã bị nhà mạng thu hồi để phục hồi mật khẩu các loại tài khoản thông qua OTP gửi về SIM điện thoại (SIM cũ của người dùng đã bỏ nhưng vẫn còn liên kết với Facebook, Zalo, Ngân hàng, iCloud). Đối tượng sử dụng các số này để yêu cầu "Quên mật khẩu", nhận mã OTP từ đó chiếm đoạt toàn bộ tài khoản và dữ liệu nhạy cảm. Ngoài ra các email cũ (lâu không đăng nhập) cũng bị chúng dùng phần mềm dò mật khẩu để tìm kiếm thông tin khôi phục tài khoản.

- Giải pháp khắc phục: (1) Rà soát ngay mục "Thông tin liên hệ" trên Zalo, Facebook, Ngân hàng... và gỡ bỏ ngay các số điện thoại/email không còn sử dụng. (2) Chuyển phương thức nhận mã xác thực từ SMS sang các ứng dụng bảo mật chuyên dụng như Google Authenticator hoặc Microsoft Authenticator. (3) Khi thay đổi số điện thoại phải thực hiện thủ tục thay đổi số điện thoại trên tất cả các dịch vụ ngân hàng và mạng xã hội trước khi bỏ SIM.

**1.3.** Cảnh báo mã độc "NFC-Stealer" đánh cắp thông tin thẻ ngân hàng qua ứng dụng giả mạo

- Mức độ: Đặc biệt nghiêm trọng.

- Mô tả: Lợi dụng quy định về xác thực sinh trắc học và cập nhật thông tin căn cước công dân, đối tượng gửi đường link qua Zalo/SMS giả mạo ứng dụng của Bộ Công an hoặc Ngân hàng. Khi cài đặt mã độc này yêu cầu người dùng áp thẻ Căn cước gắn chip hoặc thẻ Ngân hàng vào mặt sau điện thoại (qua giao tiếp NFC). Mã độc sẽ âm thầm sao chép toàn bộ dữ liệu chip và thông tin thanh toán, đồng thời chiếm quyền điều khiển điện thoại để tự động thực hiện các lệnh chuyển tiền mà người dùng không hề hay biết.

- Giải pháp khắc phục: (1) Tuyệt đối không cài đặt ứng dụng qua đường link gửi từ người lạ hoặc các tệp .APK rời. Chỉ cài đặt ứng dụng từ CH Play hoặc App Store. (2) Cơ quan Công an và Ngân hàng không làm việc qua Zalo hay yêu cầu người dùng tự quét NFC qua ứng dụng lạ. (3) Nếu đã cài đặt lập tức tắt kết nối mạng, tháo SIM và mang điện thoại đến trung tâm bảo mật để quét sạch mã độc hoặc khôi phục cài đặt gốc.

**2. Cảnh báo nghiêm trọng thông qua hệ thống quản trị mã độc tập trung EDR trên địa bàn tỉnh**

**2.1.** Cảnh báo mã độc chiếm quyền điều khiển qua tệp lối tắt giả mạo (Trojan.WinLNK.Runner.ip)

- Mức độ: Nghiêm trọng.

- Mô tả: Đây là biến thể mới nhất của dòng Trojan.WinLNK.Runner chuyên lạm dụng các tệp lối tắt (.LNK) để đánh lừa người dùng. Mã độc thường ngụy

trang dưới dạng các tài liệu PDF, thư mục ảnh hoặc tệp nén gửi qua email/USB. Khi người dùng nhấn vào thay vì mở tài liệu, nó sẽ thực thi các lệnh ẩn (PowerShell hoặc CMD) để kết nối với máy chủ điều khiển (C&C), từ đó tải xuống các loại mã độc nguy hiểm khác như backdoor hoặc mã độc đánh cắp thông tin tài chính. Kỹ thuật này giúp tin tặc dễ dàng vượt qua các hàng rào phòng thủ của phần mềm diệt virus truyền thống[1].

- Giải pháp khắc phục: Bật tính năng hiển thị đuôi tệp tin (File name extensions) trong File Explorer để nhận diện các tệp có đuôi lạ .lnk. Cảnh giác với các tệp tin nhận từ nguồn lạ qua email/USB. Quản trị viên cần cấu hình chính sách (GPO) để hạn chế hoặc giám sát việc thực thi PowerShell/CMD từ các tiến trình không xác định và luôn bật phần mềm diệt virus Smart IR.

**2.2.** Cảnh báo mã độc lây nhiễm qua file Excel (Virus.MSExcel.Laroux-based)

- Mức độ: Nghiêm trọng.

- Mô tả: Đây là loại macro-virus lây lan qua các file Microsoft Excel, đặc biệt phát tán mạnh qua ứng dụng Zalo. Khi người dùng mở file và bật tính năng "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 tống tiền (ransomware)[2].

- Giải pháp khắc phục: (1) Đối với quản trị viên hệ thống cần cấu hình Group Policy để vô hiệu hóa hoặc cảnh báo nghiêm ngặt việc thực thi macro trong các văn bản Office. (2) Đối với người dùng tuyệt đối không bấm "cho phép nội dung hoạt động" (Enable Content) hoặc "cho phép Macros" (Enable Macros) đối với các tệp tin nhận được từ nguồn không tin cậy và luôn bật phần mềm diệt virus Smart IR.

**2.3.** Cảnh báo mã độc lây nhiễm qua file AutoCAD (Virus.Acad.Bursted.a, Trojan.Acad.Agent.a)

- Mức độ: Nghiêm trọng.

- Mô tả: Đây là loại 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[3].

---

[1] Tại **Thông báo lỗ hổng bảo mật tháng 3/2026** ghi nhận mã độc này hiện đang lây nhiễm mạnh tại đơn vị Trung tâm Văn hóa Truyền thông Đức Thọ (ghi nhận gần 2.300 cảnh báo lây nhiễm), Công an tỉnh đã đề nghị đơn vị Trung tâm Văn hóa Truyền thông Đức Thọ xử lý, khắc phục và báo cáo về Công an tỉnh trước ngày 05/4/2026. Tuy nhiên đến ngày 14/4/2026 vẫn còn ghi nhận việc lây nhiễm mã độc này tại Trung tâm Văn hóa Truyền thông Đức Thọ, đề nghị đơn vị khẩn trương khắc phục và báo cáo kết quả về Công an tỉnh trước ngày **05/5/2026.**

[2] Ghi nhận lây nhiễm tại: Sở Công thương; Phường Thành Sen|Trường Mầm non Thạch Hưng; Xã Thạch Hà|Trạm y tế Thị Trấn; Sở Giáo dục và Đào tạo|THPT Can Lộc. Trong đó Trạm y tế xã Thạch Hà ghi nhận đến gần 10.000 cảnh báo liên quan đến loại mã độc này, đề nghị đơn vị Trạm y tế xã Thạch Hà xử lý, khắc phục và báo cáo về Công an tỉnh trước ngày **05/5/2026.**

[3] Ghi nhận lây nhiễm tại: Sở Xây dựng; Ban quản lý khu kinh tế; Xã Việt Xuyên; Thanh tra tỉnh; Xã Can Lộc; Xã Toàn Lưu; Phường Nam Hồng Lĩnh; Phường Nam Hồng Lĩnh. Tại **Thông báo lỗ hổng bảo mật tháng 3/2026** ghi nhận Sở Xây dựng đã bị lây nhiễm mã độc này trong một thời gian dài nhưng chưa được xử lý, Công an tỉnh đã đề nghị Sở Xây dựng xử lý, khắc phục và báo cáo về Công an tỉnh trước ngày 05/4/2026. Tuy nhiên đến ngày

- Giải pháp khắc phục: (1) Đối với quản trị viên hệ thống cần rà soát các máy tính có cài đặt AutoCAD. Sử dụng phần mềm diệt virus để làm sạch. Kiểm tra và xóa các tệp tin độc hại (như acad.lsp, acaddoc.lsp) trong thư mục cài đặt và thư mục người dùng của AutoCAD. (2) Đối với người dùng không mở các file bản vẽ 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.

**2.3.** Cảnh báo mã độc gián điệp đánh cắp thông tin cá nhân HEUR:Trojan.Win32.Fsysna.gen

- Mức độ: Nghiêm trọng.

- Mô tả: Đây là dòng mã độc gián điệp (Trojan Spy) chuyên nghiệp. Thay vì phá hoại hệ thống ngay lập tức nó âm thầm thực hiện các hành vi: theo dõi thao tác bàn phím (keylogging) để lấy mật khẩu, trích xuất dữ liệu từ các trình duyệt (cookie, mật khẩu lưu sẵn, thẻ tín dụng) và chụp ảnh màn hình của nạn nhân. Nó liên tục biến đổi mã nguồn để tránh bị nhận diện bởi các mẫu có sẵn, chỉ có thể bị phát hiện qua phân tích hành vi. Dữ liệu bị đánh cắp thường được dùng để chiếm đoạt tài khoản ngân hàng hoặc tống tiền nạn nhân[4].

- Giải pháp khắc phục: (1) Ngay lập tức quét toàn bộ hệ thống bằng phần mềm diệt virus bản quyền (như Kaspersky, Microsoft Defender bản cập nhật mới nhất, Smart IR). (2) Đổi toàn bộ mật khẩu các tài khoản quan trọng từ một thiết bị sạch khác và kích hoạt xác thực 02 lớp (MFA). (3) Không lưu mật khẩu trực tiếp trên trình duyệt, nên sử dụng các trình quản lý mật khẩu chuyên dụng (như Bitwarden, LastPass).

**2.4.** Phát hiện một số file .exe tại các đơn vị ghi nhận hành vi nguy hiểm có thể dẫn đến tấn công mã hóa dữ liệu trong tương lai

- Mức độ: Nghiêm trọng.

- Mô tả: Một số tệp tin thực thi (.exe) tại các đơn vị có hành vi nguy hiểm, tiềm ẩn rủi ro cao đối với hệ thống thông tin. Các tệp tin này có thể được phát tán thông qua email, ứng dụng nhắn tin (Zalo, Telegram,…), thiết bị lưu trữ USB hoặc tải về từ Internet.

Khi người dùng vô tình thực thi (chạy) các file .exe, 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 đặc biệt là tiền đề cho các cuộc tấn công mã hóa dữ liệu tống tiền (ransomware) trong tương lai[5].

---

28/4/2026 vẫn còn ghi nhận việc lây nhiễm mã độc này, đề nghị Sở Xây dựng khẩn trương khắc phục và báo cáo về Công an tỉnh trước ngày 05/5/2026.

[4] Ghi nhận lây nhiễm tại: Sở Nông nghiệp và Môi trường|Văn phòng Đăng ký đất đai huyện Thạch Hà-Lộc Hà; Sở Nông nghiệp và Môi trường|Vườn Quốc gia Vũ Quang.

[5] Ghi nhận lây nhiễm tại: Sở Y tế|Bệnh viện Lộc Hà; Xã Hà Linh|Trường THCS Hà Linh; Sở Nông nghiệp và Môi trường|Văn phòng đăng ký đất đai Thị xã Kỳ Anh; Sở Giáo dục và Đào tạo|THPT Cẩm Xuyên; Xã Can Lộc|Trường THCS Xuân Diệu; Sở Giáo dục và Đào tạo|Trung tâm GDTX Cẩm Xuyên; Sở Giáo dục và Đào tạo|Trường Cao đẳng y tế Hà Tĩnh.

- Giải pháp khắc phục: (1) Đối với quản trị viên hệ thống cần rà soát, kiểm tra và loại bỏ ngay các file .exe không rõ nguồn gốc trên máy trạm và máy chủ. Cấu hình Group Policy hoặc các giải pháp Endpoint Security để hạn chế hoặc chặn việc thực thi file .exe từ các thư mục không an toàn (Downloads, Temp, USB,…). Triển khai và cập nhật đầy đủ phần mềm diệt virus Smart IR cho hệ thống. (2) Đối với người dùng cần tuyệt đối không mở hoặc chạy các file .exe nhận được từ email, ứng dụng nhắn tin hoặc nguồn không rõ ràng. Không tải và cài đặt phần mềm, công cụ, file crack hoặc keygen từ Internet. Luôn bật phần mềm diệt virus Smart IR và kịp thời báo cáo bộ phận công nghệ thông tin khi phát hiện cảnh báo bất thường.

Khi phát hiện dấu hiệu tấn công mạng đề nghị các đơn vị, địa phương liên hệ Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, số điện thoại: 099.338.6777) để được phối hợp, hỗ trợ xử lý.

Công an tỉnh thông báo các đơn vị, địa phương biết, đề nghị khẩn trương rà soát, xử lý các virus, mã độc và các lỗ hổng bảo mật trên hệ thống./.

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

**KT. GIÁM ĐỐC**
**PHÓ GIÁM ĐỐC**

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

**Thượng tá Nguyễn Quốc Hùng**