BỘ CÔNG AN
CÔNG AN TỈNH HÀ TĨNH

Số: 1178/CAT-ANM

V/v thông báo lỗ hổng bảo mật nghiêm trọng tháng 3/2026

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

Hà Tĩnh, ngày 02 tháng 4 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 3/2026 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 chiến dịch lừa đảo chiếm quyền tài khoản Zalo qua hình thức "Bình chọn cuộc thi"

- Mức độ: Đặc biệt nghiêm trọng.

- Mô tả: Đây là phương thức tấn công lừa đảo đang xảy ra diện rộng trên địa bàn tỉnh Hà Tĩnh. Kẻ tấn công gửi các đường link giả mạo cuộc thi ảnh, bình chọn tài năng nhí... qua tin nhắn Zalo. Khi nạn nhân nhấn vào link và đăng nhập để "bình chọn", kẻ tấn công sẽ chiếm được mã OTP hoặc phiên đăng nhập để kiểm soát tài khoản. Sau đó đối tượng mạo danh chủ tài khoản để nhắn tin mượn tiền, lừa đảo người thân trong danh bạ hoặc tiếp tục phát tán link mã độc để mở rộng mạng lưới nạn nhân.

- Ảnh hưởng: Tất cả người dùng ứng dụng Zalo trên nền tảng Android, iOS và máy tính chưa kích hoạt bảo mật hai lớp.

- Giải pháp khắc phục: (1) Tuyệt đối không nhấn vào các đường link lạ, đặc biệt là các yêu cầu đăng nhập lại tài khoản Zalo. (2) Kích hoạt xác thực 02 lớp. (3) Thường xuyên vào mục "Lịch sử đăng nhập" để đăng xuất khỏi các thiết bị lạ. (4) Xác thực trực tiếp: Nếu nhận được tin nhắn mượn tiền, phải gọi điện thoại video và các hình thức tương tự khác để xác nhận danh tính trước khi chuyển khoản.

1.2. Cảnh báo tấn công chiếm đoạt Facebook/Messenger bằng Deepfake và link "Tin buồn/Lộ clip"

- Mức độ: Rất nghiêm trọng.

- Mô tả: Tương tự như kịch bản Zalo nhưng ở cấp độ tinh vi hơn. Kẻ tấn công gửi các link gắn tiêu đề gây sốc (tin buồn gia đình, lộ clip nhạy cảm) để đánh cắp thông tin đăng nhập Facebook. Sau khi chiếm quyền điều khiển, đối tượng sử dụng công nghệ AI Deepfake để giả dạng hình ảnh và giọng nói của chủ tài khoản thực hiện các cuộc gọi video ngắn với người thân nhằm mục đích vay tiền. Công nghệ Deepfake khiến nạn nhân dễ tin tưởng hơn vì thấy đúng khuôn mặt và nghe đúng giọng nói của người thân.

- Giải pháp khắc phục: (1) Thiết lập thêm tính năng xác thực 02 yếu tố (2FA) bằng ứng dụng tạo mã (như Google Authenticator) thay vì chỉ dùng SMS. (2) Thiết lập danh sách "Liên hệ tin cậy" để lấy lại tài khoản khi bị sự cố. (3) Khi nhận cuộc gọi video hỏi mượn tiền mà hình ảnh chập chờn, giọng nói ngắt quãng hoặc yêu cầu chuyển tiền vào số tài khoản lạ (không trùng tên) cần ngắt máy và liên lạc qua kênh khác để kiểm tra.

1.3. Cảnh báo mã độc chiếm quyền điều khiển điện thoại (Accessibility Service) giả mạo ứng dụng Chính phủ

- Mức độ: Rất nghiêm trọng.

- Mô tả: Đây là hình thức lừa đảo nguy hiểm nhất, đối tượng dẫn dụ người dùng qua Zalo/Facebook để cài đặt các tệp tin lạ (.APK) giả mạo ứng dụng VNeID, Tổng cục Thuế hoặc Cổng dịch vụ công. Sau khi cài đặt, mã độc sẽ xin quyền "Accessibility Service" (Hỗ trợ tiếp cận). Nếu người dùng đồng ý, kẻ tấn công sẽ chiếm toàn bộ quyền điều khiển điện thoại từ xa, tự động đọc mã OTP ngân hàng, theo dõi thao tác bàn phím và âm thầm chuyển tiền khỏi tài khoản ngân hàng của nạn nhân mà không cần tương tác trực tiếp.

- 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) Kiểm tra quyền ứng dụng: Vào Cài đặt > Hỗ trợ tiếp cận, tắt tất cả các ứng dụng lạ đang sử dụng quyền này. (3) Nếu nghi ngờ đã cài nhầm mã độc: Ngay lập tức ngắt kết nối Internet (Wifi/4G), khôi phục cài đặt gốc của điện thoại (Factory Reset) và thực hiện đổi mật khẩu ngân hàng, Zalo, Facebook trên một thiết bị sạch khác.

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. 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) 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.

- 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)[1]. Trong đó Ủy ban nhân dân xã Đan Hải ghi nhận đến gần 18.000 cảnh báo liên quan đến loại mã độc này, đề nghị đơn vị Ủy ban nhân dân xã Đan Hải xử lý, khắc phục và báo cáo về Công an tỉnh trước ngày 05/4/2026.

- 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[2]. Trong đó tại Sở Xây dựng ghi nhận đã bị lây nhiễm mã độc

---

[1] Ghi nhận lây nhiễm tại: Sở Công thương; Sở Y tế|Trung tâm y tế Cẩm Xuyên; Xã Cẩm Hưng|Trường Tiểu học Cẩm Hưng; Phường Thành Sen|Trạm y tế Nam Hà; Phường Thành Sen; Phường Thành Sen|Trường Mầm non Thạch Hưng; Xã Thạch Xuân|Trạm y tế Thạch Xuân; Xã Thạch Hà|Trạm y tế Thị Trấn; Sở Y tế|Bệnh viện Sức khỏe Tâm thần; Xã Thạch Hà|Trường Mầm Non Thạch Long; Xã Đan Hải.

[2] Ghi nhận lây nhiễm tại: Sở Xây dựng; Xã Toàn Lưu; Xã Kỳ Xuân.

này trong một thời gian dài nhưng chưa được xử lý, đề nghị Sở Xây dựng xử lý, khắc phục và báo cáo về Công an tỉnh trước ngày 05/4/2026.

- 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[3]. Trong đó tại Ủy ban nhân dân xã Kỳ Xuân ghi nhận đến gần 1.800 cảnh báo liên quan đến loại mã độc này, đề nghị Ủy ban nhân dân xã Kỳ Xuân xử lý, khắc phục và báo cáo về Công an tỉnh trước ngày 05/4/2026.

- 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 2 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

[3] Ghi nhận lây nhiễm tại: Xã Thiên Cầm; Xã Kỳ Xuân.

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[4].

- 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, 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

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

Thượng tá Nguyễn Quốc Hùng

[4] Ghi nhận lây nhiễm tại: Sở Giáo dục và Đào tạo|Trung tâm GDTX Cẩm Xuyên; Sở Giáo dục và Đào tạo|Trường Cao đẳng y tế Hà Tĩnh; Sở Nông nghiệp và Môi trường|Văn phòng đăng ký đất đai; Sở Y tế|Bệnh viện Sức khỏe Tâm thần; Xã Gia Hanh.