Ký bởi: CÔNG AN TỈNH HÀ TĨNH
Email: cat@hatinh.bca
Ngày ký: 06-03-2026 16:06:40 +07:00

BỘ CÔNG AN
CÔNG AN TỈNH HÀ TĨNH

Số: 785/CAT-ANM

V/v thông báo lỗ hổng bảo mật nghiêm trọng tháng 02/2026

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

Hà Tĩnh, ngày 05 tháng 3 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 02/2026 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 lỗ hổng thực thi mã từ xa nghiêm trọng trong Dịch vụ cổng máy tính từ xa của Microsoft (Remote Desktop Gateway)

- Mức độ: Đặc biệt nghiêm trọng.

- Mô tả: Microsoft vừa công bố khẩn cấp lỗ hổng bảo mật mới trong các máy chủ thư điện tử Exchange Server. Lỗ hổng này cho phép kẻ tấn công (đã có quyền truy cập thấp hoặc chiếm được một tài khoản email thông thường) thực hiện kỹ thuật leo thang đặc quyền để chiếm quyền kiểm soát toàn bộ máy chủ (Domain Controller). Nguy hiểm hơn, mã khai thác (PoC) của lỗ hổng này đã bị lộ lọt và đang được các nhóm ransomware sử dụng để tấn công mã hóa dữ liệu các doanh nghiệp.

- Phiên bản ảnh hưởng: Microsoft Exchange Server 2016, 2019 và các phiên bản Exchange Hybrid chưa cập nhật bản vá "Patch Tuesday" tháng 02/2026.

- Giải pháp khắc phục: Quản trị viên các hệ thống cần cài đặt ngay bản cập nhật bảo mật (Security Update) tháng 02/2026 mà Microsoft vừa phát hành ngày 10/02/2026. Nếu chưa thể cập nhật ngay, cần kích hoạt tính năng "Extended Protection" (bảo vệ mở rộng) trên máy chủ Exchange và rà soát lại

nhật ký truy cập để phát hiện các dấu hiệu đăng nhập bất thường từ các địa chỉ IP lạ.

1.2. Cảnh báo chiến dịch phát tán mã độc giả mạo "Phần mềm thuế và tài liệu nội bộ đầu năm"

- Mức độ: Rất nghiêm trọng.

- Mô tả: Lợi dụng thời điểm các doanh nghiệp quay trở lại làm việc và chuẩn bị cho kỳ quyết toán thuế đầu năm, các nhóm tin tặc đang đẩy mạnh hai hình thức tấn công nhắm vào khối văn phòng: (1) Giả mạo cơ quan thuế gửi email hoặc tin nhắn Zalo mạo danh cán bộ thuế, yêu cầu kế toán hoặc chủ doanh nghiệp tải về "Phần mềm hỗ trợ kê khai thuế 2026" hoặc cập nhật ứng dụng "eTax Mobile" bản mới nhất để không bị phạt. Đường link dẫn đến một website giả mạo và tải xuống file chứa mã độc gián điệp (spyware). (2) Giả mạo tài liệu nội bộ gửi email giả danh lãnh đạo hoặc phòng nhân sự với tiêu đề gây tò mò như "Kế hoạch kinh doanh mới sau Tết 2026", "Quy chế lương thưởng và nhân sự mới áp dụng từ tháng 02/2026",... Các file đính kèm (Word, Excel, PDF) chứa mã độc tàng hình, sẽ kích hoạt ngay khi người dùng mở file và bấm "Enable Content" (bật nội dung).

- Giải pháp khắc phục: (1) Quán triệt cán bộ trong đơn vị tuyệt đối không tải phần mềm thuế qua các đường link lạ hoặc các file chia sẻ qua Zalo. Chỉ truy cập vào website chính thống của Tổng cục Thuế (gdt.gov.vn) hoặc các kho ứng dụng chính thức (CH Play, App Store). Cảnh báo nhân viên không được tùy tiện mở các file đính kèm có nội dung lạ hoặc thúc giục về thời gian và cần kiểm tra kỹ địa chỉ email nguồn. Tuyệt đối không bấm "Enable Editing" hoặc "Enable Content" (macro) trên các file Office nếu không chắc chắn về độ an toàn. (2) Tăng cường phổ biến rộng rãi thủ đoạn lừa đảo mới này đến toàn thể cán bộ, công chức, viên chức, đặc biệt là những người làm công tác tài chính, kế toán.

1.3. Lỗ hổng nghiêm trọng trong các thiết bị lưu trữ mạng (NAS) phổ biến

- Mức độ: Đặc biệt nghiêm trọng.

- Mô tả: Một lỗ hổng thực thi mã từ xa (RCE) vừa được phát hiện trong hệ điều hành của các thiết bị lưu trữ NAS, lỗ hổng nằm trong module chia sẻ file qua giao thức SMB/AFP. Tin tặc có thể quét các thiết bị NAS kết nối Internet, khai thác lỗ hổng để xóa sạch dữ liệu hoặc mã hóa toàn bộ file backup nhằm đòi tiền chuộc.

- Phiên bản ảnh hưởng: Các thiết bị NAS của Synology, QNAP chạy phiên bản hệ điều hành cũ chưa cập nhật bản vá ngày 15/02/2026.

- Giải pháp khắc phục: (1) Tiến hành rà soát và lập tức ngắt kết nối các thiết bị NAS khỏi mạng Internet công cộng (không public IP trực tiếp, không mở Port Forwarding), chỉ cho phép truy cập qua VPN nội bộ. (2) Đăng nhập trang quản trị thiết bị và cập nhật lên phiên bản Firmware mới nhất ngay lập tức. Kích hoạt xác thực 02 bước (2FA) cho tài khoản quản trị NAS.

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 lây lan Worm.Win32.AutoRun.fnc

- Mức độ: Nghiêm trọng.

- Mô tả: Worm.Win32.AutoRun.fnc là mã độc dạng sâu máy tính (worm) được viết trên nền tảng Win32, có khả năng tự sao chép và phát tán mạnh mẽ qua các thiết bị lưu trữ di động (USB) và ổ đĩa mạng thông qua tệp tin cấu hình autorun.inf. Mã độc thường ngụy trang dưới dạng các tệp thực thi hệ thống hoặc ẩn mình trong các thư mục gốc để đánh lừa người dùng. Sau khi xâm nhập, nó chỉnh sửa khóa Registry để tự động khởi động cùng hệ thống, tạo cửa sau (backdoor) và có khả năng phát tán liên kết độc hại qua các ứng dụng nhắn tin. Mã độc này làm suy yếu bảo mật hệ thống, gây mất dữ liệu và tạo điều kiện cho tin tặc chiếm quyền điều khiển từ xa[1].

- Giải pháp khắc phục: (1) Đối với quản trị viên hệ thống cần sử dụng các công cụ rà quét mã độc chuyên dụng như Smart IR, Kaspersky Virus Removal Tool hoặc Microsoft Safety Scanner để quét toàn bộ hệ thống. Kiểm tra và xóa bỏ các tệp lạ như system3_.exe hoặc autorun.inf trên các phân vùng đĩa. Thực hiện cấu hình Group Policy để vô hiệu hóa hoàn toàn tính năng AutoRun hoặc AutoPlay trên toàn bộ máy trạm. (2) Đối với người dùng thực hiện quét virus trước khi mở USB, mở tài liệu, 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.

---

[1] Ghi nhận lây nhiễm tại: Sở Văn hoá Thể thao và Du lịch|Văn phòng Sở Văn hóa Thể thao và Du lịch.

[2] Ghi nhận lây nhiễm tại: Sở Tài chính|Văn phòng Sở Tài chính; Xã Cổ Đạm|Trường Tiểu học Cổ Đạm; Xã Sơn Hồng; Xã Tứ Mỹ; Xã Toàn Lưu; Xã Sơn Tây; Xã Can Lộc; Xã Sơn Kim 1; Xã Đức Đồng; Sở Công thương; Xã Hương Sơn; Xã Tiên Điền; Xã Mai Phụ; Xã Kim Hoa.

- 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].

- 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 Worm.Win32.FakeDoc (lây lan qua USB và các tệp tin giả mạo)

- Mức độ: Nghiêm trọng.

- Mô tả: Đây là loại sâu máy tính (worm) chủ yếu lây lan tự động qua các thiết bị lưu trữ USB, bên cạnh đó còn có thể lây lan qua các kênh khác như Zalo, Email. Nó tạo ra các tệp tin thực thi (.exe) giả mạo dưới dạng các tài liệu quen thuộc (Word, Excel, PDF,...) và ẩn đi các tệp tin thật. Khi người dùng mở tệp giả mạo mã độc sẽ được kích hoạt, gây ra nguy cơ lây lan trên diện rộng trong mạng nội bộ và tạo backdoor cho tin tặc xâm nhập sâu hơn vào hệ thống, từ đó có thể thực hiện các kịch bản tấn công nguy hiểm hơn như tấn công mã hóa dữ liệu (Ransomware)[4].

- Giải pháp khắc phục: (1) Đối với quản trị viên hệ thống cần rà soát, cách ly các máy tính có dấu hiệu nhiễm, sử dụng Group Policy để vô hiệu hóa tính năng AutoRun đối với các thiết bị USB. (2) Đối với người dùng cần quét virus tất cả các thiết bị USB trước khi sử dụng, bật chế độ hiển thị file ẩn để phát hiện các tệp tin đáng ngờ. Đặc biệt phải cẩn trọng với các tệp tin gửi qua Zalo, Email có biểu tượng tài liệu nhưng có đuôi là ".exe" hoặc là dạng "Shortcut" và luôn bật phần mềm diệt virus Smart IR.

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: Rất 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: Sở Xây dựng; Xã Can Lộc; Xã Toàn Lưu; Sở Nông nghiệp và Môi trường; Xã Gia Hanh; Xã Thạch Hà.

[4] Ghi nhận lây nhiễm tại: Xã Thượng Đức.

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].

- 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.

2.5. Phát hiện dấu hiệu lộ lọt thông tin cá nhân trên không gian mạng

- Mức độ: Rất nghiêm trọng.

- Mô tả: Phát hiện một số thông tin, dữ liệu nhạy cảm của người dân trên địa bàn tỉnh Hà Tĩnh có dấu hiệu bị lộ lọt trên không gian mạng.

- Giải pháp khắc phục: Quán triệt nghiêm túc việc xử lý văn bản, tài liệu chứa thông tin cá nhân của người dân, yêu cầu tuân thủ nghiêm túc quy định của Luật bảo vệ dữ liệu cá nhân 2025 và các quy định khác có liên quan. Không chia sẻ dữ liệu cá nhân của người dân qua các ứng dụng OTT (như Facebook, Zalo, Telegram,...) hoặc tải lên AI (như Chatgpt, Gemini, Deepseek,...). Đặc biệt các đơn vị, địa phương có trách nhiệm trong xử lý dữ liệu phục vụ bầu cử ĐBQH khóa XVI và đại biểu HĐND các cấp nhiệm kỳ 2026 - 2031 cần tuân thủ nghiêm túc việc bảo vệ dữ liệu cá nhân trong quá trình thực hiện nhiệm vụ.

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

[5] Ghi nhận lây nhiễm tại: Sở Nông nghiệp và Môi trường|Văn phòng Đăng ký đất đai huyện Thạch Hà-Lộc Hà; Xã Trường Lưu; Sở Giáo dục và Đào tạo|THPT Nguyễn Văn Trỗi; Xã Cẩm Duệ; Viện kiểm sát nhân dân|Viện kiểm sát nhân dân tỉnh; Sở Y tế|Bệnh viện Lộc Hà.