

**BỘ CÔNG AN
CÔNG AN TỈNH HÀ TĨNH**

Số 2662/CAT-ANM

V/v thông báo lỗ hổng bảo mật
nghiêm trọng tháng 6/2026

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

Hà Tĩnh, ngày 29 tháng 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 6/2026 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. Rò rỉ thông tin cá nhân từ việc thanh lý thiết bị cũ (Ổ cứng, Máy tính, Điện thoại)

- Mức độ: Nghiêm trọng.

- Mô tả: Người dùng có thói quen bán lại hoặc vứt bỏ các thiết bị hỏng, cũ (laptop, ổ cứng rời, thẻ nhớ, điện thoại) mà chỉ xóa dữ liệu theo cách thông thường (Delete/Format) hoặc chưa xử lý vì máy không lên nguồn. Thực tế, dữ liệu vẫn tồn tại trên chip nhớ và có thể được khôi phục bằng các phần mềm chuyên dụng. Các đối tượng thu mua đồ cũ có thể trích xuất hình ảnh nhạy cảm, thông tin căn cước công dân, mật khẩu trình duyệt hoặc tệp tin công ty để tống tiền, giả mạo danh tính hoặc rao bán trên “chợ đen”.

- Giải pháp ứng phó: ⁽¹⁾ Trước khi bán, cần thực hiện việc ghi đè dữ liệu (Zero Fill) hoặc khôi phục cài đặt gốc nhiều lần. ⁽²⁾ Với thiết bị hỏng không thể bật nguồn nhưng chứa dữ liệu nhạy cảm, tốt nhất nên tiêu hủy vật lý (phá hỏng hoàn toàn chip nhớ/phiên đĩa) thay vì bán phế liệu. ⁽³⁾ Luôn mã hóa ổ đĩa (BitLocker trên Windows hoặc FileVault trên Mac) ngay từ khi bắt đầu sử dụng để đảm bảo dù bị lấy mất ổ cứng, kẻ gian cũng không thể đọc được nội dung.

1.2. Phần mềm độc hại “Camera ảo” và thiết bị can thiệp vượt sinh trắc học

- Mức độ: Đặc biệt nghiêm trọng (vô hiệu hóa lớp bảo mật khuôn mặt).

- Mô tả: Đối tượng sản xuất các phần mềm độc hại hoặc bán các điện thoại đã bị can thiệp phần cứng. Các công cụ này tạo ra một “Camera ảo”, cho phép chúng chèn các video Deepfake hoặc ảnh chân dung tĩnh của nạn nhân vào quy trình quét khuôn mặt của App ngân hàng. Thay vì quét khuôn mặt thật, hệ thống bị lừa nhận diện dữ liệu từ tệp tin có sẵn, giúp kẻ gian thực hiện lệnh chuyển tiền trái phép.

- Giải pháp ứng phó: ⁽¹⁾ Tuyệt đối không cài đặt các ứng dụng từ nguồn lạ (file .APK) ngoài kho ứng dụng chính thống (Google Play/App Store). ⁽²⁾ Không sử dụng các điện thoại đã bị bẻ khóa (Root/Jailbreak) hoặc mua máy cũ không rõ nguồn gốc đã bị can thiệp phần cứng. ⁽³⁾ Cần trọng khi cung cấp ảnh chân dung, video khuôn mặt trên các ứng dụng giải trí, bói toán không uy tín trên mạng.

1.3. Nguy cơ mất an toàn thông tin và rủi ro pháp lý từ phần mềm Office, Windows “Bẻ khóa” (Crack/Key lậu)

- Mức độ: Nghiêm trọng (Dễ bị cài cắm mã độc và đối mặt với án hình sự).

- Mô tả: Việc sử dụng các công cụ kích hoạt trái phép (Crack, Key lậu, Activator) để dùng miễn phí Windows, Office... căn cứ theo mức độ có thể là hành vi vi phạm pháp luật hình sự. Bên cạnh đó, các công cụ này thường chứa mã độc, phần mềm gián điệp (spyware) âm thầm hoạt động. Khi cài đặt, chúng có thể tạo “cửa sau” (backdoor) cho phép hacker toàn quyền kiểm soát máy tính, đánh cắp thông tin đăng nhập ngân hàng, dữ liệu doanh nghiệp và biến máy tính của bạn thành công cụ tấn công mạng.

- Giải pháp ứng phó: ⁽¹⁾ Chỉ sử dụng phần mềm có bản quyền chính hãng từ nhà sản xuất; tuyệt đối không sử dụng các công cụ bẻ khóa hoặc mua “Key lậu” giá rẻ trên mạng. ⁽²⁾ Đối với doanh nghiệp và tổ chức, cần thường xuyên rà soát, kiểm tra bản quyền phần mềm trên máy tính nhân viên để tránh rủi ro bị truy cứu trách nhiệm hình sự về. ⁽³⁾ Ưu tiên sử dụng các phần mềm mã nguồn mở hoặc các bộ công cụ miễn phí có uy tín nếu không muốn trả phí bản quyền.

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 nhiễm tệp tin đa hình và chiếm quyền điều khiển (Virus.Win32.Virut.ce và Virus.Win64.Moiva.a)

- Mức độ: Đặc biệt nghiêm trọng (nguy cơ hỏng toàn bộ hệ thống và mất dữ liệu).

- Mô tả: Đây là một trong những dòng virus nguy hiểm nhất thuộc loại “File Infector” (lây nhiễm tệp tin). Khác với các loại mã độc thông thường, Virut.ce tự động chèn mã độc vào toàn bộ các tệp thực thi (.exe, .scr) có trên máy tính, bao gồm cả các tệp tin cốt lõi của hệ điều hành Windows. Điểm cực kỳ nguy hiểm là tính chất “đa hình” (polymorphic): virus tự thay đổi cấu trúc mã nguồn của nó sau mỗi lần lây nhiễm, khiến các phần mềm diệt virus thông thường rất khó nhận diện triệt để. Khi hoạt động, nó mở “cửa sau” (backdoor) để kết nối tới máy chủ điều

hiển (C&C), cho phép tin tặc chiếm toàn quyền kiểm soát máy tính, đánh cắp thông tin mật và sử dụng máy tính của nạn nhân để thực hiện các cuộc tấn công mạng khác (Botnet). Virus này lây lan với tốc độ chóng mặt qua các loại ổ cứng di động, USB, thẻ nhớ,... và các thư mục chia sẻ chung trong mạng nội bộ (LAN)¹.

- Giải pháp khắc phục: ⁽¹⁾ Khi có dấu hiệu nhiễm (máy chạy chậm bất thường, các ứng dụng .exe bị lỗi không mở được), lập tức ngắt kết nối mạng Internet và rút toàn bộ các thiết bị lưu trữ ngoài (USB, ổ cứng rời) để ngăn chặn virus gửi dữ liệu ra ngoài và lây lan sang máy khác. ⁽²⁾ Không nên cố gắng diệt virus bằng các phần mềm chạy trực tiếp trên Windows vì Virut.ce thường tìm cách vô hiệu hóa hoặc lây nhiễm ngược vào chính phần mềm diệt virus đó. Thay vào đó, hãy sử dụng các đĩa cứu hộ chuyên dụng (Rescue Disk) để quét mã độc từ môi trường bên ngoài hệ điều hành (Boot qua USB/CD). ⁽³⁾ Do đặc tính lây nhiễm sâu vào mọi tệp tin thực thi, việc “quét và diệt” thường làm hỏng tệp gốc khiến ứng dụng không thể hoạt động ổn định. Giải pháp an toàn và triệt để nhất là thực hiện sao lưu dữ liệu quan trọng (chỉ sao lưu file tài liệu như docx, pdf, xlsx; tuyệt đối không sao lưu file .exe), sau đó định dạng lại toàn bộ ổ cứng (Format) và cài đặt lại hệ điều hành mới. ⁽⁴⁾ Trước khi cài đặt, các đơn vị liên hệ đầu mối cài đặt phần mềm Smart IR² để được hướng dẫn cấp lại Key.

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

- 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)³.

- 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

¹ Ghi nhận lây nhiễm tại: Sở Giáo dục và Đào tạo/THPT Cẩm Xuyên với gần 300 cảnh báo lây nhiễm; Xã Sơn Kim 2 với gần 3.600 cảnh báo lây nhiễm.

Đề nghị các đơn vị xử lý, khắc phục và báo cáo về Công an tỉnh trước ngày 10/7/2026.

² Liên hệ VNPT anh Đặng Quốc Sinh (số điện thoại 0975357960) là đầu mối cài đặt phần mềm Smart IR.

³ Ghi nhận lây nhiễm tại: Ban Tổ chức Tỉnh ủy; Sở Y tế/Văn phòng Sở y tế; Sở Y tế/Trung tâm y tế Cẩm Xuyên; Sở Y tế/Chi cục Dân số; Sở Y tế/Trung tâm y tế Thạch Hà; Sở Y tế/Trung tâm y tế Tiên Điền; Sở Nội vụ/Ban dân tộc - Tôn giáo; Sở Công thương/Văn phòng Sở công thương; Sở Nông nghiệp và Môi trường/Vườn Quốc gia Vũ Quang; Xã Kỳ Khang; Phường Nam Hồng Lĩnh; Xã Kim Hoa; Xã Mai Hoa; Xã Tứ Mỹ; Xã Hương Sơn; Xã Sơn Kim 2; Xã Hương Sơn/Trường THCS Trung Phú; Xã Cẩm Lạc; Xã Sơn Tây; Xã Sơn Hồng; Xã Sơn Giang/Trường THCS Hải Thượng Lãn Ông; Xã Đồng Tiến/Trạm y tế Thạch Hội; Xã Đồng Tiến/Trạm y tế Thạch Văn; Xã Hà Linh/Trường THCS Hà Linh; Xã Thạch Khê/UBND-Đảng ủy-MTTQ-TTHCC xã Thạch Khê; Xã Thạch Hà/UBND-Đảng ủy-MTTQ-TTHCC; Xã Đông Kinh/UBND-Đảng ủy-MTTQ-TTHCC xã Đông Kinh; Xã Đan Hải Trong đó Sở Nội vụ/Ban dân tộc - Tôn giáo; Sở Y tế/Văn phòng Sở y tế; Sở Y tế/Trung tâm y tế Cẩm Xuyên; Xã Sơn Giang/Trường THCS Hải Thượng Lãn Ông; Xã Kim Hoa; Xã Mai Hoa; Xã Tứ Mỹ; Xã Hương Sơn; Xã Sơn Hồng ghi nhận nhiễm loại mã độc này nhiều nhất.

Đề nghị các đơn vị xử lý, khắc phục và báo cáo về Công an tỉnh trước ngày 10/7/2026.

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 phần mềm AutoCAD

- 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 trọng⁴.

- 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, acadoc.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.

2.4. 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 lai⁵.

- 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.

⁴ Ghi nhận lây nhiễm tại: Sở Nông nghiệp và Môi trường/Văn phòng Đăng ký đất đai huyện Cẩm Xuyên; đặc biệt ghi nhận lây nhiễm hơn 1.500 lần tại xã Hương Sơn. Công an tỉnh đề nghị xã Hương Sơn xử lý, khắc phục và báo cáo về Công an tỉnh trước ngày 10/7/2026.

⁵ Ghi nhận lây nhiễm tại: Sở Xây dựng; Sở Y tế/Bệnh viện Sức khỏe Tâm thần; Xã Can Lộc; Xã Cổ Đàm. Công an tỉnh đề nghị các đơn vị xử lý, khắc phục và báo cáo về Công an tỉnh trước ngày 10/7/2026.

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**

Thượng tá Nguyễn Quốc Hùng