

Công an Hà Tĩnh cảnh báo hoạt động tấn công bằng mã độc ransomware

16:42 07/01/2026

Thời gian qua, lợi dụng hoạt động chuyển đổi số, tin tặc tăng cường tấn công bằng mã độc tống tiền (ransomware) với thủ đoạn hết sức tinh vi, gây thiệt hại đặc biệt nghiêm trọng cho hệ thống thông tin của các cơ quan, đơn vị trên địa bàn tỉnh.

Theo Công an tỉnh Hà Tĩnh, hiện nay, các cuộc tấn công có xu hướng nhằm vào các lĩnh vực trọng yếu như y tế, giáo dục, tài chính... và mã độc liên tục được phát triển với nhiều biến thể. Đáng chú ý như mimic ransomware, có khả năng xâm nhập sâu vào hệ thống máy chủ, mã hóa dữ liệu và đánh cắp thông tin nhạy cảm.

Việc bị tấn công bằng mã độc ransomware không chỉ gây tê liệt hệ thống thông tin, mất mát dữ liệu không thể phục hồi mà còn ảnh hưởng trực tiếp đến an ninh, kinh tế, quyền và lợi ích hợp pháp của người dân.



Trong tháng 12 vừa qua, Công an tỉnh Hà Tĩnh đã tổ chức diễn tập thực chiến, bảo đảm an toàn thông tin mạng

Từ công tác hướng dẫn, kiểm tra, Công an tỉnh Hà Tĩnh đánh giá, các cơ quan, đơn vị trên địa bàn còn nhiều tồn tại, sơ hở trong triển khai công tác đảm bảo an ninh mạng, an toàn thông tin, là điều kiện để tin tặc lợi dụng tấn công mạng, trong đó có hoạt động tấn công bằng ransomware.

Cụ thể là chưa triển khai cài đặt phần mềm giám sát, phát hiện và phản ứng mã độc tập trung (EDR) trên hệ thống máy chủ và các thiết bị máy trạm quan trọng; hệ thống máy chủ chưa được trang bị đầy đủ các giải pháp bảo mật chuyên dụng; chưa được kết nối, giám sát tập trung qua “Trung tâm giám sát an ninh mạng tỉnh Hà Tĩnh - SOC”; tình trạng cài đặt các phần mềm cho phép truy cập vào hệ thống máy chủ từ xa (remote desktop, SSH, VPN...) và đặt mật khẩu yếu, dễ đoán; một số tài khoản có dấu hiệu bị lộ, lọt nhưng chưa được thay đổi, xử lý kịp thời; không kiểm tra thời hạn bản quyền của các thiết bị bảo mật quan trọng (tường lửa, antivirus...) dẫn đến tình trạng hết hạn hỗ trợ kỹ thuật, không được gia hạn, nâng cấp kịp thời; một số hệ thống máy chủ, máy trạm không có bản quyền hệ điều hành, không được cập nhật các bản vá lỗi bảo mật định kỳ; tình trạng cài đặt, sử dụng phần mềm không có bản quyền, không rõ nguồn gốc, phần mềm bẻ khóa (cracked), phần mềm giả mạo vẫn diễn ra phổ biến.

Để đảm bảo an ninh dữ liệu, an toàn thông tin, Công an tỉnh Hà Tĩnh đề nghị, các cơ quan, đơn vị thực hiện nghiêm túc quy trình ứng cứu sự cố khẩn cấp khi phát hiện dấu hiệu hoạt động tấn công mạng, cụ thể khi phát hiện máy tính có các dấu hiệu bất thường như bị mã hóa dữ liệu (biểu tượng file bị thay đổi, không thể mở được file), xuất hiện các tệp tin đòi tiền chuộc, hoạt động chậm bất thường, chuyên trách công nghệ thông tin tại các cơ quan, đơn vị cần thực hiện theo các bước như sau:

Cách ly: Rút dây cắm mạng LAN và ngắt kết nối wifi của máy tính nghi bị nhiễm. Nếu sự cố xảy ra trên diện rộng thì cần ngắt kết nối internet của toàn bộ hệ thống (ngắt kết nối trên router/switch tổng).

Giữ nguyên hiện trạng: Không tắt máy tính bằng lệnh shutdown, tiến hành ngắt nguồn điện trực tiếp (rút phích cắm hoặc giữ nút nguồn) để bảo toàn các dấu vết trong bộ nhớ RAM phục vụ điều tra, truy vết.

Báo cáo: Thông báo Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, số điện thoại: 0993.386.777) để được hướng dẫn, phối hợp xử lý. Tuyệt đối không tự ý xử lý sự cố, không cố gắng khôi phục dữ

liệu, không trả tiền chuộc cho tin tặc khi chưa có sự phối hợp của cơ quan chức năng.

Triển khai đầy đủ các giải pháp bảo mật và dự phòng cho hệ thống thông tin như: rà soát, cài đặt đầy đủ phần mềm giám sát mã độc tập trung (EDR) trên toàn bộ máy chủ và các máy trạm trọng yếu; đăng ký giám sát an toàn thông tin tập trung qua hệ thống SOC của tỉnh; thay đổi mật khẩu các tài khoản có quyền quản trị hệ thống, tài khoản truy cập từ xa theo chính sách an toàn (độ dài tối thiểu 8 ký tự, có chữ hoa, chữ thường, chữ số, ký tự đặc biệt...) và triển khai cơ chế thay đổi mật khẩu định kỳ;

Bắt buộc kích hoạt xác thực đa yếu tố (MFA) đối với các truy cập từ bên ngoài internet; thường xuyên rà soát gia hạn, cập nhật, nâng cấp bản quyền đối với các thiết bị, phần mềm bảo mật (firewall, antivirus,...), hệ điều hành, office, đảm bảo các thiết bị, phần mềm có bản quyền và được cập nhật bản vá bảo mật mới nhất;

Gỡ bỏ triệt để các phần mềm không rõ nguồn gốc, phần mềm bẻ khóa; sao lưu dữ liệu dự phòng thường xuyên theo nguyên tắc 3-2-1 (tạo 3 bản sao lưu, 2 trên các phương tiện lưu trữ khác nhau, 1 bản sao lưu ngoại tuyến, không kết nối với hệ thống).

Khánh Trình