BỘ CÔNG AN
CÔNG AN TP HẢI PHÒNG

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

Số: 1011 /CAHP-ANM
V/v thông báo tình hình an toàn, an ninh mạng tháng 4/2025

Hải Phòng, ngày 23 tháng 04 năm 2025

Kính gửi:
- Các cơ quan Đảng thành phố;
- Các cơ quan Trung ương tổ chức theo ngành dọc;
- Các Sở, ban, ngành;
- Các Quận ủy, Huyện ủy, UBND các quận, huyện;
- Các đơn vị sự nghiệp Thành phố;
- Các tổ chức chính trị, xã hội, doanh nghiệp.

Thực hiện nhiệm vụ quản lý nhà nước về an toàn, an ninh mạng trên địa bàn thành phố, Công an thành phố Hải Phòng thông báo về tình hình an ninh mạng và kết quả hoạt động của công tác giám sát an ninh mạng như sau:

- Ngày 27/3/2025, website uy tín về an ninh mạng "https://thehackernews.com" thông báo về việc các nhà nghiên cứu đã phát hiện 150.000 trang web bị xâm phạm thông qua hình thức tấn công Javascript injection, nhằm quảng bá các nền tảng cờ bạc trực tuyến có trụ sở tại Trung Quốc. Các hacker đã chèn mã độc vào các trang web để chuyển hướng người dùng hoặc hiển thị quảng cáo không mong muốn. Cuộc tấn công nhằm vào các trang web chưa cập nhật bảo mật. Các chuyên gia khuyến cáo quản trị viên trang web nên vá lỗ hổng, theo dõi mã nguồn cẩn thận.

- Ngày 26/3/2025, chuyên trang uy tín về an ninh mạng "https://bleepingcomputer" thông báo về lỗ hổng zero-day CVE-2025-1234 ảnh hưởng đến công cụ JavaScript V8 của trình duyệt Google Chrome, cho phép tin tặc thực thi mã từ xa trên các thiết bị mục tiêu. Chiến dịch khai thác nhắm vào các nhân vật cấp cao trong chính phủ và các tổ chức quan trọng. Lỗ hổng trên hiện đã được vá và các chuyên gia khuyên người dùng khẩn trương cập nhật lên phiên bản mới nhất của trình duyệt Google Chrome để tránh bị tin tặc khai thác, tấn công.

- Ngày 24/3/2025, Hiệp hội An ninh mạng Việt Nam (NCA) công bố 04 lỗ hổng bảo mật nghiêm trọng trên nền tảng xác thực tập trung WSO2, cho phép tin tặc dễ dàng sử dụng thành chuỗi khai thác để chiếm đoạt tài khoản quản trị ứng dụng và chiếm quyền máy chủ, xâm nhập hạ tầng nội bộ, truy cập thông tin nhạy cảm. Các giải pháp của WSO2 được sử dụng rộng rãi và đóng vai trò trọng

yếu trong hệ thống thông tin của các cơ quan bộ, ban, ngành, tỉnh thành tại Việt Nam, cụ thể là các hệ thống Trục tích hợp dữ liệu (LGSP) và Hệ thống Đăng nhập một lần (SSO). Do đó, các lỗ hổng bảo mật này có nguy cơ ảnh hưởng đến nhiều cơ quan, tổ chức, bộ ban ngành. NCA đề nghị các đơn vị, cơ quan, tổ chức có sử dụng giải pháp WSO2 nhanh chóng kiểm tra mức độ ảnh hưởng và cập nhật bản vá mới nhất của WSO2 để phòng, chống các cuộc tấn công khai thác lỗ hổng bảo mật đã biết.

- Kaspersky khu vực Châu Á – Thái Bình Dương ghi nhận trung bình 80 vụ tấn công mã độc tống tiền (ransomware) mỗi ngày vào các tổ chức, doanh nghiệp tại Việt Nam, trong đó có tập đoàn CMC. Đây là mã độc mã hóa dữ liệu với mục đích đòi tiền chuộc để giải mã dữ liệu. Kaspersky khuyến cáo: "Bộ phận IT nên tắt các cổng và dịch vụ không sử dụng để giảm thiểu bề mặt tấn công và hạn chế điểm yếu. Việc sao lưu dữ liệu và kiểm tra khả năng khôi phục cần thực hiện thường xuyên để giảm thiểu thiệt hại từ tấn công ransomware".

- Trong tháng 4/2025 đã phát hiện các lỗ hổng bảo mật của hệ điều hành Window đáng chú ý như sau: Lỗ hổng CVE-2025-26663 cho phép thực thi mã từ xa qua khai thác cơ chế "use-after-free" của Windows Lightweight Directory Access Protocol (LDAP); Lỗ hổng CVE-2025-26686 cho phép thực thi mã từ xa lợi dụng quá trình khóa bộ nhớ trong ngăn xếp TCP/IP của Windows khiến dữ liệu bị phơi bày trong bộ nhớ, tạo cơ hội tấn công từ xa; Lỗ hổng CVE-2025-27480 cho phép thực thi mã từ xa, lợi dụng lỗ hổng trong tính năng Remote Desktop của Window; Lỗ hổng bảo mật CVE-2025-27491 cho phép thực thi mã từ xa tận dụng lỗi của Window Hyper-V; Lổ hổng bảo mật CVE-2025-27745 cho phép kẻ xấu thực hiện nhiều phương thức tấn công, lợi dụng lỗi trong phân bổ và giải phóng bộ nhớ của phần mềm Microsoft Office. Hiện tại Microsoft đã phát hành bản vá cho các lỗ hổng bảo mật trên. Quản trị viên, người dùng Window nên khẩn trương cài đặt các bản cập nhật mới nhất của Window để bảo đảm an toàn.

- Trong tháng 4/2025, Hệ thống quản lý mã độc tập trung của thành phố đã phát hiện 100 thiết bị thuộc 28 tổ chức trên địa bàn thành phố Hải Phòng bị nhiễm mã độc, với tổng cộng 48 loại mã độc đính kèm trong 1265 file. Công an thành phố đã phát hiện, phối hợp với Viettel thông báo và xử lý 03 trường hợp mất an ninh mạng, an toàn thông tin đối với Trung tâm dữ liệu thành phố và Trung tâm thông tin truyền thông thuộc Sở Khoa học và công nghệ.

CATP Hải Phòng đề nghị các sở, ban, ngành, tổ chức trên địa bàn thành phố thực hiện nghiêm các quy định về bảo đảm an toàn, an ninh mạng trên địa bàn thành phố. Quá trình thực hiện nếu có khó khăn, vướng mắc đề nghị liên hệ về CATP *(Qua Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao; địa chỉ: Số 55 Bến Bính, Hồng Bàng, Hải Phòng; SĐT: 069.278.5415)* để được hướng dẫn, hỗ trợ./.

Nơi nhận:
- Như trên;
- Đ/c Giám đốc CATP (để báo cáo);
- Lưu VT; ANM(Đ4).

TL.GIÁM ĐỐC
TRƯỞNG PHÒNG ANM
VÀ PCTP SỬ DỤNG CNC

Thượng tá Đinh Trọng Chiềm