BỘ CÔNG AN
CÔNG AN TP HẢI PHÒNG

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

Số: 4194/CAHP-ANM
V/v thông báo tình hình an toàn, an ninh mạng tháng 10/2025

Hải Phòng, ngày 29 tháng 10 năm 2025

Kính gửi:

- Các cơ quan Đảng thành phố;
- Các cơ quan Trung ương đóng tại địa phương;
- Các Sở, ban, ngành;
- UBND các xã, phường, đặc khu;
- 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 trong tháng 10/2025 như sau:

- Microsoft cảnh báo về việc tin tặc đang lợi dụng nền tảng Teams để thu thập thông tin, lừa người dùng chia sẻ dữ liệu nhạy cảm, mạo danh nguồn tin cậy và phát tán mã độc qua tin nhắn và cuộc gọi, đồng thời dùng Teams để duy trì truy cập và thực hiện trộm dữ liệu. Teams đang trở thành mục tiêu giá trị trong chu trình tấn công, do đó người dùng cần tăng cường bảo vệ danh tính, bảo mật điểm cuối và các biện pháp phòng thủ mạng khác.

- Hiệp hội an ninh mạng Việt Nam (NCA) phát hiện và thu thập các mẫu mã độc giả mạo ứng dụng Chính phủ và ngân hàng nhắm mục tiêu vào người dùng Android tại Việt Nam. Đây là một biến thể của mã độc đã được phát hiện từ 2016 có mục đích thu thập và đánh cắp thông tin đăng nhập của người dùng.

- NCA cảnh báo về hoạt động sử dụng mã độc RUST CHAOSBOT tấn công vào các hệ thống thông tin tại Việt Nam. Chiến dịch này sử dụng mồi nhử liên quan đến các tổ chức tài chính, ngân hàng để phát tán mã độc mới ChaosBot và lợi dụng Discord làm máy chủ C2. Quản trị viên cần theo dõi sát sao log hệ thống, kịp thời phát hiện các kết nối bất thường đến các máy chủ khả nghi.

- Trong tháng 10/ 2025, các công ty an ninh mạng đã công bố các lỗ hổng bảo mật sau:

+ Oracle đã phát hành bản vá bảo mật khẩn cấp cho Oracle E-Business Suite phiên bản từ 12.2.3 đến 12.2.14 để khắc phục lỗ hổng CVE-2025-61884 có thể bị khai thác từ xa và truy cập dữ liệu nhạy cảm, đồng thời cảnh báo khách hàng áp dụng sớm và tiếp tục duy trì các phiên bản được hỗ trợ.

+ Microsoft phát hành bản vá khắc phục 167 lỗ hổng bảo mật, trong đó có 08 lỗ hổng zero day, bao gồm các lỗ hổng liên quan đến leo thang đặc quyền, thực thi mã từ xa và bypass bảo mật. Các lỗ hổng được sửa liên quan đến Window

Modem driver, Remote Access…

+ Microsoft cảnh báo về việc hai lỗ hổng trên Window là CVE-2025-49708 và CVE-2025-55315 liên quan đến Secure Boot đang bị khai thác ngoài thực tế, cho phép tin tặc nâng cao đặc quyền, thực thi mã từ xa và vượt qua bảo mật, ảnh hưởng tới mọi phiên bản Window đã phát hành. Hiện chưa có thông tin nào về việc Microsoft đã phát hành bản vá đối với lỗ hổng này.

+ Lỗ hổng nghiêm trọng trong bộ định tuyến TP-Link AX1800 có mã định danh CVE-2023-28760 cho phép tin tặc trên cùng một mạng LAN thực hiện thực thi mã độc từ xa dưới quyền root. Mã khai thác đã được công khai, do đó người dùng cần cân nhắc thay đổi thiết bị hoặc chờ bản cập nhật mới nhất của nhà sản xuất.

+ Oracle đã công bố bản vá cho ba lỗ hổng bảo mật (CVE-2025-9230, CVE-2025-9231, CVE-2025-9232), trên nhiều phiên bản thư viện, trong đó CVE-2025-2031 có thể cho phép khôi phục khóa riêng tư và từ đó thực thi mã hoặc tấn công DoS, hai lỗ hổng còn lại được đánh giá là mức độ trung bình và thấp, có khả năng gây DoS.

+ Lỗ hổng bảo mật CVE-2025-20333 và CVE-2025-20362 cho phép tin tặc thực thi mã tùy ý trên gần 50.000 thiết bị tường lửa Cisco ASA và FTD mà không cần xác thực. Cisco khuyến cáo người dùng hạn chế tiếp xúc Web VPN và tăng cường ghi nhật ký, giám sát. Quản trị viên cần nhanh chóng cập nhật và cài đặt bản vá nhằm giảm thiểu thiệt hại.

- Trong tháng 10/2025, Hệ thống quản lý mã độc tập trung của thành phố đã phát hiện 35 thiết bị thuộc 16 tổ chức trên địa bàn thành phố Hải Phòng bị nhiễm mã độc, với tổng cộng 31 loại mã độc đính kèm trong 168 file; hệ thống SOC của thành phố đã phát hiện và ngăn chặn 03 trường hợp các IP lạ không rõ nguồn gốc thực hiện hành vi rà quét lỗ hổng và thực thi mã bất thường trên các trang website của thành phố; Qua công tác quản lý và nắm tình hình, Công an thành phố chưa phát hiện vụ việc mất an ninh, an toàn nào trên các Cổng thông tin điện tử của thành phố.

Công an thành phố đề nghị các sở, ban, ngành, tổ chức trên địa bàn thành phố chủ động cập nhật và nâng cấp giải pháp về bảo đảm an toàn, an ninh mạng đối với hệ thống thông tin. Quá trình thực hiện nếu có khó khăn, vướng mắc đề nghị liên hệ về Công an thành phố *(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).

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CÔNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
CÔNG AN THÀNH PHỐ HẢI PHÒNG

Đại tá Lê Đức Thành