BỘ CÔNG AN
CÔNG AN TP HẢI PHÒNG

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

Số: 5869/CAHP-ANM
V/v thông báo tình hình an toàn, an ninh mạng tháng 11/2025

Hải Phòng, ngày 29 tháng 11 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 11/2025 như sau:

- Ngày 18/11/2025, Cloudflare đã gặp phải sự cố ngừng hoạt động tồi tệ nhất trong 6 năm qua, gây ra gián đoạn hoạt động trên nhiều trang web và nền tảng trực tuyến trong gần 6 giờ (trong đó có nền tảng mạng xã hội phổ biến X (Twitter), dịch vụ ChatGPT của OpenAI, ứng dụng Canva, cổng thanh toán Paypal, ứng dụng Uber Eats…). Công ty cho biết sự cố xảy ra sau khi thay đổi kiểm soát quyền truy cập cơ sở dữ liệu, dẫn đến lỗi lan rộng trên mạng Global Network của nhà cung cấp dịch vụ này. Vấn đề này không phải do sự cố tấn công mạng hay hoạt động độc hại nào gây ra, nguyên nhân gốc là tệp cấu hình lỗi bị sao chép trên nhiều hệ thống, dẫn đến hiệu ứng domino làm sập hệ thống và trả về mã trạng thái 5xx.

- Các chuyên gia cảnh báo về chiến dịch lừa đảo dựa trên cơ chế mời doanh nghiệp của Facebook/Meta, khi tin tặc gửi email giả mời từ tên miền hợp pháp @facebookmail.com để dẫn người nhận đến các trang thu thập thông tin đăng nhập, nhằm nhắm tới các doanh nghiệp dựa vào Meta Marketing; Hệ thống ghi nhận khoảng 40.000 email lừa đảo và phạm vi tiếp cận rộng, nhắm đến nhiều ngành và khu vực, bằng cách mạo danh thương hiệu và sử dụng hạ tầng của Meta Business Suite để tăng tính tin cậy.

- Tin tặc đang dùng RedTiger, công cụ kiểm tra thâm nhập mã nguồn mở, để phát triển một mã độc đánh cắp thông tin (infostealer) nhắm vào Discord và dữ liệu thanh toán, đồng thời có thể lấy dữ liệu trình duyệt, ví tiền điện tử, tài khoản trò chơi và ảnh chụp màn hình. Mã độc này hoạt động bằng cách đóng gói thành tập tin nhị phân độc lập, quét các tệp Discord và trình duyệt, đánh cắp token và dữ liệu người dùng, sau đó chèn JavaScript tùy chỉnh vào Discord để bắt các sự kiện đăng nhập và thanh toán, trước khi nén dữ liệu và gửi lên GoFile qua Discord webhook.

- Các nhà nghiên cứu an ninh mạng đã phát hiện một tiện ích mở rộng độc hại của Chrome đóng giả làm ví Ethereum hợp pháp có tên "Safery: Ethereum Wallet" đánh lừa người dùng bằng quảng cáo ví an toàn để quản lý ETH nhưng thực chất lại chứa backdoor đánh cắp Seed của ví Ethereum, thực hiện các giao dịch vi mô với các ví do tin tặc kiểm soát nhằm rút sạch tài khoản của người dùng mà không cần máy chủ C2.

- Trong tháng 11/2025, các công ty an ninh mạng đã công bố các lỗ hổng bảo mật sau:

+ Các nhà nghiên cứu vừa phát hiện ra một lỗ hổng nghiêm trọng trong công cụ kết xuất đồ họa Blink của Chromium, công nghệ đứng đằng sau các trình duyệt Chrome, Edge, Brave, Opera và hầu hết các trình duyệt sử dụng công nghệ Chromium khác. Lỗ hổng được đặt tên là Brash, không cần khai thác mã độc phức tạp, chỉ vài dòng JavaScript được nhúng trong một trang web độc hại do tin tặc tự xây dựng là đủ khiến trình duyệt sập, đồng thời ngốn toàn bộ CPU, làm treo cả hệ thống. Hacker có thể nhúng đoạn mã này vào trang web, hoặc hẹn giờ kích hoạt trong những thời điểm quan trọng, gây tê liệt các hệ thống web vận hành thời gian thực như tài chính, y tế hay tự động hóa doanh nghiệp. Người dùng nên tránh truy cập các trang web lạ, đáng ngờ cho đến khi có bản vá chính thức; giới hạn việc chạy mã không tin cậy trong môi trường trình duyệt, đặc biệt là các ứng dụng dựa trên Chromium.

+ Lỗ hổng CVE-2025-64095 là lỗ hổng nghiêm trọng nhưng lại khá dễ khai thác cho phép tải lên tệp mà không cần xác thực trên nền tảng quản lý nội dung web phổ biến DNN (DotNetNuke) phiên bản trước 10.1.1. Lỗ hổng nằm ở trình soạn thảo HTML mặc định, nơi kiểm tra và xác minh việc tải tệp chưa được thực hiện đúng cách, cho phép kẻ tấn công tải các tệp độc hại hoặc ghi đè lên các tệp quan trọng trên hệ thống mà không cần thông tin đăng nhập. Người dùng cần cập nhật bản vá bảo mật cho DNN, tăng cường giám sát và sẵn sàng có phương án xử lý khi phát hiện có dấu hiệu khai thác, tấn công mạng.

+ Microsoft vừa phát hành bản vá khắc phục 63 lỗ hổng bảo mật, trong đó có: CVE-2025-55315, một lỗ hổng nghiêm trọng trong nền tảng ASP.NET Core, công nghệ đang vận hành hàng triệu website và dịch vụ trực tuyến trên toàn cầu. Lỗi này cho phép kẻ tấn công khai thác kỹ thuật HTTP Request Smuggling, khiến hệ thống xử lý sai lệch các yêu cầu HTTP và vô hiệu hóa các cơ chế bảo mật. Với mức độ nguy hiểm cao và khả năng khai thác dễ dàng, CVE-2025-55315 được đánh giá là một trong những lỗ hổng ASP.NET Core đáng lo ngại nhất năm 2025; Lỗ hổng bảo mật zeroday đang được khai thác CVE-2025-62215 liên quan đến race condition trong Windows Kernel, cho phép leo thang đặc quyền cục bộ…Ngoài ra bản vá này còn bao gồm các lỗ hổng nghiêm trọng khác gồm lỗ hổng RCE, tiết lộ thông tin, Ddos và Spoofing.

+ Các nhà nghiên cứu bảo mật tại Google Threat Intelligence Group (GTIG) đã phát hiện ra nhóm tin tặc UNC6485 nhắm mục tiêu vào máy chủ Triofox phiên bản 16.4.10317.56372 bằng cách khai thác lỗ hổng nghiêm trọng CVE-2025-12480 trong nền tảng chia sẻ tệp và truy cập từ xa để thực thi mã từ xa

với quyền SYSTEM. Quản trị viên hệ thống cần áp dụng bản cập nhật mới nhất có trong phiên bản 16.10.10408.56683 được phát hành vào ngày 14/10, đồng thời kiểm tra tài khoản quản trị và công cụ diệt Virus của Triofox có được thiết lập để chạy các tập lệnh hoặc tệp nhị phân trái phép hay không.

+ Lỗ hổng zero-day chưa từng được biết đến trong phần mềm thư viện của Samsung libimagecodec.quram.so xử lý hình ảnh, vừa được phát hiện và theo dõi với mã CVE-2025-21042 cho phép tin tặc cài phần mềm gián điệp LANDFALL vào thiết bị mà người dùng không cần làm gì, thậm chí không cần nhấp vào liên kết.

+ Tháng 11 đánh dấu sự trở lại của nhiều loại mã độc nguy hiểm: Sau khi chiến dịch Endgame bị phá vỡ, mã độc DanaBot đã hoạt động trở lại sau 6 tháng gián đoạn với biến thể mới (phiên bản 669) dùng cơ sở hạ tầng C2 từ Tor và kết nối ngược, tiếp tục nhắm mục tiêu vào thông tin đăng nhập, ví tiền điện tử…; Cũng trong tháng 11, mã độc DarkComet RAT vừa bị phát hiện bằng cách ngụy trang trong các ứng dụng ví BitCoin giả và chương trình giao dịch, được đóng gói dưới dạng UPX và phân phối qua tệp RAR để né tránh bộ lọc bảo mật, nhằm ghi lại phím và thu thập thông tin đăng nhập từ nạn nhân, đồng thời có thể giúp tin tặc truy cập từ xa và duy trì hoạt động trên máy nạn nhân.

- Trong tháng 11/2025, Hệ thống quản lý mã độc tập trung của thành phố đã phát hiện 31 thiết bị thuộc 15 tổ chức trên địa bàn thành phố Hải Phòng bị nhiễm mã độc, với tổng cộng 34 loại mã độc đính kèm trong 171 file; hệ thống SOC của thành phố chưa phát hiện hành vi bất thường, độc hại trên các trang website của thành phố; Qua công tác quản lý và nắm tình hình, Công an thành phố đã phát hiện tình trạng mất an ninh mạng, an toàn thông tin đối với một số cổng thông tin điện tử của thành phố; Công an thành phố đã thông báo và phối hợp với các đơn vị trên để làm rõ trách nhiệm, kịp thời khắc phục.

Công an thành phố Hải Phòng 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

Đại tá Lê Đức Thành