BỘ CÔNG AN
CÔNG AN TP HẢI PHÒNG

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

Số: 4834/CAHP-ANM
V/v thông báo tình hình lợi dụng hoạt động lấy ý kiến dự thảo văn kiện Đại hội XIV của Đảng gây mất an toàn, an ninh mạng

Hải Phòng, ngày 03 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 mất an ninh mạng khẩn cấp như sau:

1. Cảnh báo mã độc nguy hiểm lợi dụng việc góp ý dự thảo văn kiện đại hội XIV của đảng

- Thời gian qua, Bộ Chính trị tiến hành tổ chức lấy ý kiến Nhân dân đối với dự thảo văn kiện Đại hội XIV của Đảng. Lợi dụng tình hình trên, các thế lực thù địch, đối tượng xấu đã lợi dụng việc này để thực hiện các hoạt động phá hoại, vụ lợi. Đặc biệt, lực lượng Công an đã phát hiện mã độc Valley RAT liên kết đến địa chỉ máy chủ điều khiển (C2): 27.124.9.13, port 5689, được ẩn giấu trong tệp có tên *"Dự thảo nghị quyết đại hội.exe"*. Kẻ xấu lợi dụng hoạt động lấy ý kiến dự thảo nghị quyết để lừa người dùng cài đặt, thực hiện các hành vi nguy hiểm như đánh cắp thông tin nhạy cảm, chiếm đoạt tài khoản cá nhân, đánh cắp tài liệu, phát tán mã độc sang các máy tính khác.

- Kết quả phân tích cho thấy mã độc sau khi được cài vào máy tính người dùng sẽ tự động thực thi mỗi khi khởi động máy, kết nối đến máy chủ điều khiển từ xa do tin tặc chiếm giữ, từ đó tiếp tục thực hiện các hành vi nguy hiểm nói trên. Ngoài ra, lực lượng Công an còn phát hiện các tập tin mã độc khác có kết nối đến máy chủ C2 mà tin tặc đã phát tán trong thời gian gần đây gồm: *"Báo cáo tài chính2.exe"; "Thanh toán bảo hiểm doanh nghiệp.exe"; "Công văn hỏa tốc của chính phủ.exe"; "Hỗ trợ kê khai thuế.exe"; "Công văn đánh giá hoạt động đảng.exe"; "Mẫu giấy ủy quyền.exe"; "Biên bản báo cáo quý III.exe"*.

2. Biện pháp phòng ngừa

Công an thành phố Hải Phòng đề nghị các sở, ban, ngành, tổ chức trên địa bàn thành phố nâng cao cảnh giác, không tải, cài đặt, mở các tập tin không rõ nguồn gốc (đặc biệt các tập tin thực thi có đuôi .exe, .dll, .bat, .msi,…) và thực

hiện các biện pháp kỹ thuật sau để phòng chống tấn công:

- Rà soát hệ thống thông tin của đơn vị, địa phương để phát hiện các tập tin nghi ngờ; nếu ghi nhận sự cố, cách ly máy bị nhiễm, ngắt kết nối Internet và báo cáo về Công an thành phố (Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao) để được hỗ trợ; quét toàn bộ hệ thống bằng phần mềm bảo mật cập nhật mới nhất (EDR/XDR) có khả năng phát hiện và diệt mã độc ẩn.

** Khuyến nghị sử dụng: Avast, AVG, Bitdefender (bản free) hoặc Windows Defender cập nhật mới nhất;* ***lưu ý:*** *Kaspersky bản free hiện chưa phát hiện được mã độc này.*

- Rà quét thủ công hệ thống: Kiểm tra trên Process Explorer, nếu thấy tiến trình không có chữ ký số hoặc giả mạo tên tập tin văn bản thì cần cách ly ngay và sử dụng các công cụ quét để kiểm tra; Kiểm tra tcpview để xem kết nối mạng - nếu phát hiện kết nối về IP 27.124.9.13 thì cần xử lý ngay; khẩn trương block trên firewall, ngăn chặn truy cập đến địa chỉ IP độc hại 27.124.9.13.

Công an thành phố Hải Phòng thông báo để các sở, ban, ngành, tổ chức trên địa bàn thành phố được biết. 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 X.H.C.N VIỆT NAM
CÔNG AN THÀNH PHỐ HẢI PHÒNG

Đại tá Lê Đức Thành