SAO Y; CÔNG AN THÀNH PHỐ HẢI PHÒNG; Thời gian ký: 2025-05-27T17:29:29+07:00

BỘ CÔNG AN
CÔNG AN TP HẢI PHÒNG

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

Số: 868[a]/CAHP-ANM
V/v thông báo tình hình an toàn, an ninh mạng tháng 5/2025

Hải Phòng, ngày 24 tháng 05 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 30/4/2025, nhiều trang Web uy tín về an ninh mạng đã đưa tin về việc Cục điều tra liên bang Mỹ thông báo danh sách hơn 42.000 tên miền lừa đảo liên quan đến dịch vụ LabHost. Đây là một trong những mạng lưới cung cấp tài nguyên cho các chiến dịch phishing quy mô lớn, giúp tin tặc tạo và quản lý các trang Web giả mạo nhằm đánh cắp dữ liệu nhạy cảm của người dùng. Các doanh nghiệp, tổ chức, cá nhân có thể tải về danh sách này từ đường link "https://www.ic3.gov/CSA/2025/LabHost_Domains.csv" để nắm được, từ đó nhận diện, chặn truy cập cũng như tăng cường cảnh báo về các mối đe doạ từ LabHost, góp phần phòng tránh, hạn chế thiệt hại do các chiến dịch lừa đảo trực tuyến gây ra.

- Ngày 28/4/2025, Website "https://thehackernews.com" thông báo về việc nhóm tin tặc Earth Kurma nhắm mục tiêu vào Đông Nam Á bằng Rootkit và các công cụ đánh cắp dữ liệu trên nền tảng đám mây. Nhóm này đã tận dụng mã độc tinh vi để ẩn mình, kiểm soát hệ thống nạn nhân và thu thập thông tin nhạy cảm, khiến các tổ chức tại Đông Nam Á, trong đó có cả các cơ quan truyền thông, chính phủ của Việt Nam, đối mặt với nguy cơ bị rò rỉ dữ liệu nghiêm trọng.

- Ngày 05/5/2025, Website "https://thehackernews.com" thông báo về việc phát hiện lỗ hổng trong tính năng Airplay của Apple cho phép tin tặc xâm nhập và kiểm soát hoàn toàn thiết bị Apple mà không cần người dùng tương tác trực tiếp. Người dùng cần khẩn trương cập nhật hệ điều hành IOS lên phiên bản mới nhất để tránh bị tin tặc khai thác, tấn công.

- Ngày 06/5/2025, trang Web chính thức của Tiki đã bị tin tặc tấn công, tự động chuyển hướng sang một trang Web cờ bạc. Nguyên nhân chính là do vấn đề cấu hình hoặc đăng ký tên miền không đúng cách, dẫn đến mất kiểm soát và tạo điều kiện cho các trang Web độc hại hoặc giả mạo khai thác. Sự cố này làm ảnh hưởng đến uy tín của Tiki và gây hoang mang cho người dùng, đồng thời

một lần nữa nhấn mạnh tầm quan trọng của việc quản lý tên miền chặt chẽ để đảm bảo an toàn.

- Trong tháng 05/2025, các nhà nghiên cứu đã phát hiện lỗ hổng nghiêm trọng đối với thư viện WebDriverManager, là thành phần thiết yếu trong bộ công cụ Selenium, một bộ công cụ phổ biến dùng để tự động hoá kiểm thử, thực thi chức năng trên Website. Lỗ hổng XXE này có mã định danh là CVE-2025-4641, lợi dụng chính sách tham chiếu đến XML bên ngoài không phù hợp, cho phép tin tặc đánh cắp dữ liệu nhạy cảm, thực thi mã độc hoặc gây ra các tác động tiêu cực khác. Quản trị viên, lập trình viên nên cài đặt, sử dụng các phiên bản ổn định cũ hơn của Selenium, bao gồm cả WebDriverManager, để phục vụ nhu cầu công việc cho đến khi bản vá được phát hành.

- Trong tháng 05/2025, Microsoft đã phát hành bản vá đối với 78 lỗ hổng bảo mật trên hệ điều Windows, trong đó có 11 lỗ hổng được xếp hạng rất nghiêm trọng, 66 lỗ hổng nghiêm trọng, và có 05 lỗ hổng Zero-day đã và đang được tội phạm khai thác là: CVE-2025-30397 khai thác lỗ hổng của Microsoft Scripting Engine khi truy cập tài nguyên sử dụng kiểu không tương thích, cho phép thực thi mã độc từ xa qua mạng; CVE-2025-30400 khai thác lỗ hổng cho phép sử dụng bộ nhớ mặc dù đã được free của Windows DWM, giúp tin tặc nâng quyền trái phép trong nội bộ; CVE-2025-32701 và CVE-2025-32706 khai thác lỗ hổng cho phép sử dụng bộ nhớ sau khi free của Windows Common Log File System Driver, giúp tin tặc nâng quyền trái phép trong nội bộ; CVE-2025-32709 khai thác lỗ hổng cho phép sử dụng bộ nhớ mặc dù đã được free của Windows Ancillary Function Driver cho WinSock, giúp tin tặc nâng quyền trái phép trong cục bộ. Quản trị viên, người dùng Window nên khẩn trương cài đặt các bản cập nhật mới nhất của Window để bảo đảm an toàn.

- Từ ngày 16/4/2025 - 15/5/2025, Hiệp hội An ninh mạng quốc gia Việt Nam đã phát hiện hoạt động tấn công, mã hoá, đòi tiền chuộc nhằm vào các nền tảng ảo hoá tại nhiều đơn vị ở Việt Nam do nhóm tin tặc Harley Quinn, một nhóm ransomware mới, được ghi nhận từ năm 2024 thực hiện. Việc xảy ra các vụ việc tấn công này một phần là do các đơn vị còn chủ quan, chưa nâng cao cảnh giác và siết chặt cơ chế quản trị truy cập vào hệ thống ảo hoá, chưa đầu tư hệ thống an ninh, bảo mật và chưa đủ nhân sự chuyên trách về an toàn, an ninh mạng. Các cuộc tấn công vào nền tảng ảo hoá thường gây ra thiệt hại lớn vì khi bị mã hoá sẽ khó khôi phục hệ thống.

- Cũng trong tháng 5/2025, Hiệp hội An ninh mạng quốc gia Việt Nam đã phát hiện nhiều mã độc đánh cắp thông tin người dùng tại Việt Nam, đều là biến thể đã được tuỳ chỉnh, làm rối mã gốc của mã độc mã nguồn mở QuasarRat, một mã độc thường xuyên được tin tặc sử dụng. Đồng thời, các mã độc này đều kết nối đến máy chủ C2 185.149.232.197 của tin tặc. Quản trị viên, người dùng cần nâng cao cảnh giác, cài đặt các chương trình AV chất lượng, đồng thời kiểm tra kỹ lưỡng trước khi chạy các file thực thi có nguy cơ cao như .exe, .bat...

- Trong tháng 5/2025, Hệ thống quản lý mã độc tập trung của thành phố đã phát hiện 124 thiết bị thuộc 27 tổ chức trên địa bàn thành phố Hải Phòng bị

nhiễm mã độc, với tổng cộng 51 loại mã độc đính kèm trong 1092 file. Công an thành phố đã phát hiện nhiều dấu hiệu mất an ninh, an toàn thông tin đối với các hệ thống thông tin trên địa bàn thành phố và đang tiếp tục xác minh, làm rõ.

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).

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

Thượng tá Đinh Trọng Chiềm

Phụ lục

DANH SÁCH CÁC ĐƠN VỊ NHẬN VĂN BẢN

(Kèm theo Công văn số /CAHP-ANM ngày /4/2025 của Công an thành phố)

1. Đơn vị có hệ thống thông tin quan trọng nhận văn bản điện tử

STT	TÊN ĐƠN VỊ
Khối các cơ quan chính quyền thành phố	
1.	Văn phòng Đoàn đại biểu Quốc hội và Hội đồng nhân dân
2.	Văn phòng Ủy ban nhân dân thành phố
3.	Sở Công Thương
4.	Sở Giáo dục và Đào tạo
5.	Sở Xây dựng
6.	Sở Tài chính
7.	Sở Khoa học và Công nghệ
8.	Sở Nội vụ
9.	Sở Ngoại vụ
10.	Sở Văn hóa, Thể thao và Du lịch
11.	Sở Nông nghiệp và Môi trường
12.	Sở Tư pháp
13.	Sở Y tế
14.	Ban Quản lý Khu kinh tế
15.	Thanh tra thành phố
Thành ủy, Quận ủy, Huyện ủy, Ủy ban nhân dân các quận, huyện, thành phố	
1.	Quận Ngô Quyền
2.	Quận Hồng Bàng
3.	Quận Đồ Sơn
4.	Quận Dương Kinh
5.	Quận Kiến An

6.	Quận Hải An
7.	Quận Lê Chân
8.	Huyện An Dương
9.	Huyện Cát Hải
10.	Huyện An Lão
11.	Huyện Tiên Lãng
12.	Thành phố Thủy Nguyên
13.	Huyện Vĩnh Bảo
14.	Huyện Kiến Thụy
15.	Huyện Bạch Long Vỹ
Khối các cơ quan Trung ương đóng trên địa bàn thành phố	
1.	Bảo hiểm xã hội khu vực VIII
2.	Bộ Chỉ huy Quân sự thành phố
3.	Bộ Chỉ huy Bộ đội biên phòng Hải Phòng
4.	Ngân hàng nhà nước Chi nhánh Khu vực 6
5.	Chi cục Thuế khu vực 3
6.	Chi cục Hải quan khu vực 3
7.	Chi cục Thống kê
8.	Cục Thi hành án dân sự thành phố
9.	Tòa án nhân dân thành phố
10.	Kho bạc Nhà nước khu vực III
Khối các cơ quan Đảng thành phố	
1.	Văn phòng Thành uỷ
2.	Ban Nội chính Thành ủy
3.	Ban Tuyên giáo và Dân vận Thành ủy
4.	Ban Tổ chức Thành ủy

5.	Ủy ban kiểm tra Thành ủy
6.	Đảng ủy các cơ quan Đảng thành phố
7.	Đảng ủy Ủy ban nhân dân thành phố
Khối các đơn vị sự nghiệp thuộc Ủy ban nhân dân thành phố	
1.	Vườn Quốc gia Cát Bà
2.	Trường Đại học Hải Phòng
3.	Trung tâm Báo chí và Truyền thông Hải Phòng
4.	Trường Cao đẳng Kỹ thuật Hải Phòng
5.	Trường Cao đẳng Y tế Hải Phòng
6.	Trường Cao đẳng Kinh tế Hải Phòng
Tổ chức chính trị, xã hội	
1.	Ủy ban Mặt trận Tổ quốc Việt Nam thành phố
2.	Liên đoàn Lao động thành phố
3.	Đoàn Thanh niên Cộng sản Hồ Chí Minh thành phố
4.	Hội Nông dân thành phố
5.	Hội Cựu chiến binh thành phố
6.	Hội Liên hiệp Phụ nữ thành phố
7.	Liên minh Hợp tác xã thành phố
8.	Liên hiệp các Hội Khoa học và Kỹ thuật thành phố
9.	Hội Chữ thập đỏ thành phố

2. Đơn vị có hệ thống thông tin quan trọng nhận bản giấy

1.	Công ty TNHH MTV điện lực Hải Phòng
2.	Cảng hàng không quốc tế Cát Bi
3.	Công ty cổ phần cấp nước Hải Phòng
4.	Công ty cổ phần Cảng Hải Phòng
5.	Viettel Hải Phòng

6.	Viễn thông Hải Phòng
7.	Viện kiểm sát nhân dân thành phố
8.	Trường Đại học Y Dược Hải Phòng
9.	Quỹ Đầu tư phát triển Hải Phòng
10.	Ban Quản lý Dự án đầu tư xây dựng công trình dân dụng và hạ tầng Hải Phòng
11.	Ban Quản lý Dự án đầu tư xây dựng các công trình giao thông và nông nghiệp Hải Phòng