UBND THÀNH PHỐ HẢI PHÒNG
SỞ GIÁO DỤC VÀ ĐÀO TẠO

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

Số: 3422 /SGDĐT-TCHC
V/v thông báo tình hình an toàn, an ninh mạng tháng 5/2025

Hải Phòng, ngày 02 *tháng* 6 *năm 2025*

Kính gửi:
- Trưởng phòng CMNV cơ quan Sở;
- Trưởng phòng GDĐT quận, huyện, thành phố Thủy Nguyên;
- Hiệu trưởng trường trung cấp, cao đẳng trên địa bàn thành phố;
- Hiệu trưởng trường THPT, PT nhiều cấp;
- Giám đốc trung tâm GDNN-GDTX quận, huyện, thành phố Thủy Nguyên;
- Thủ trưởng các đơn vị trực thuộc.

Ngày 24/5/2025, Sở Giáo dục và Đào tạo (GDĐT) nhận được Văn bản số 868a/CAHP-ANM của Công an thành phố Hải Phòng về việc thông báo tình hình an toàn, an ninh mạng tháng 5/2025 *(gửi kèm theo)*.

Căn cứ tình hình an ninh mạng tháng 4/2025 qua Thông báo của Phòng An ninh mạng - Công an thành phố Hải Phòng, Sở GDĐT đề nghị Thủ trưởng các đơn vị thực hiện nghiêm các quy định về bảo đảm an toàn, an ninh mạng cho các hệ thống thông tin thuộc phạm vi quản lý, cụ thể:

I. Tình hình an ninh mạng đáng chú ý trong tháng 5/2025:

a) Tên miền lừa đảo liên quan đến dịch vụ LabHost: Ngày 30/4/2025, Cục Điều tra Liên bang Mỹ (FBI) đã công bố danh sách hơn 42.000 tên miền lừa đảo liên quan đến dịch vụ LabHost. Đây là một 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 để đánh cắp dữ liệu nhạy cảm của người dùng. Các đơn vị có thể tải danh sách này từ đường dẫn "https://www.ic3.gov/CSA/2025/LabHost_Domains.csv" để nhận diện và chặn truy cập, tăng cường cảnh báo về các mối đe dọa từ LabHost.

b) Nhóm tin tặc Earth Kurma nhắm mục tiêu vào Đông Nam Á: Ngày 28/4/2025, nhóm tin tặc Earth Kurma được ghi nhận đã 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, bao gồm cả các cơ quan truyền thông, chính phủ của Việt Nam, đối mặt với nguy cơ bị rò rỉ dữ liệu nghiêm trọng.

c) Lỗ hổng trong tính năng Airplay của Apple: Ngày 05/5/2025, một lỗ hổng trong tính năng Airplay của Apple đã được phát hiện, cho phép tin tặc xâm

nhập và kiểm soát hoàn toàn thiết bị Apple mà không cần người dùng tương tác trực tiếp.

d) Trang web Tiki bị tấn công chuyển hướng: 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 được xác định 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 nhấn mạnh tầm quan trọng của việc quản lý tên miền chặt chẽ để đảm bảo an toàn.

đ) Lỗ hổng nghiêm trọng đối với thư viện WebDriverManager (CVE-2025-4641): Trong tháng 05/2025, các nhà nghiên cứu đã phát hiện lỗ hổng nghiêm trọng (CVE-2025-4641) đối với thư viện WebDriverManager, một thành phần thiết yếu trong bộ công cụ Selenium. Lỗ hổng XXE này 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.

e) Bản vá của Microsoft cho hệ điều hành Windows: Trong tháng 05/2025, Microsoft đã phát hành bản vá đối với 78 lỗ hổng bảo mật trên hệ điều hành Windows, trong đó có 11 lỗ hổng rất nghiêm trọng, 66 lỗ hổng nghiêm trọng, và 05 lỗ hổng Zero-day đã và đang được tội phạm khai thác. Các lỗ hổng Zero-day bao gồm:

- CVE-2025-30397: Khai thác lỗ hổng của Microsoft Scripting Engine, cho phép thực thi mã độc từ xa qua mạng.

- CVE-2025-30400: Khai thác lỗ hổng sử dụng bộ nhớ sau khi giải phóng của Windows DWM, giúp tin tặc nâng quyền trái phép trong nội bộ.

- CVE-2025-32701 và CVE-2025-32706: Khai thác lỗ hổng sử dụng bộ nhớ sau khi giải phóng của Windows Common Log File System Driver, giúp tin tặc nâng quyền trái phép trong nội bộ.

- CVE-2025-32709: Khai thác lỗ hổng sử dụng bộ nhớ sau khi giải phóng của Windows Ancillary Function Driver cho WinSock, giúp tin tặc nâng quyền trái phép trong cục bộ.

f) Tấn công mã hóa, đòi tiền chuộc nhắm vào các nền tảng ảo hóa: 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 hóa, đòi tiền chuộc nhắm vào các nền tảng ảo hóa 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. Các cuộc tấn công này gây thiệt hại lớn và khó khôi phục hệ thống.

g) Mã độc đánh cắp thông tin người dùng: Trong tháng 5/2025, Hiệp hội An ninh mạng quốc gia Việt Nam cũng phát hiện nhiều mã độc đánh cắp thông

tin người dùng tại Việt Nam, là các biến thể đã được tùy chỉnh, làm rối mã gốc của mã độc mã nguồn mở QuasarRat. Các mã độc này đều kết nối đến máy chủ C2 185.149.232.197 của tin tặc.

h) Tình hình nhiễm mã độc trên địa bàn thành phố Hải Phòng: 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.

II. CẢNH BÁO VÀ HƯỚNG DẪN GIẢI PHÁP:

Để phòng ngừa và giảm thiểu rủi ro từ các cuộc tấn công mạng, Sở Giáo dục và Đào tạo Hải Phòng đề nghị Thủ trưởng các đơn vị giáo dục khẩn trương thực hiện các biện pháp sau:

1. Chủ động cập nhật và nâng cấp giải pháp về an toàn, an ninh mạng:

- Khẩn trương cập nhật hệ điều hành iOS lên phiên bản mới nhất đối với các thiết bị Apple để tránh bị tin tặc khai thác lỗ hổng Airplay.

- Đối với quản trị viên và lập trình viên sử dụng thư viện WebDriverManager, nên cài đặt và sử dụng các phiên bản ổn định cũ hơn của Selenium, bao gồm cả WebDriverManager, cho đến khi bản vá được phát hành.

- Quản trị viên và người dùng Windows nên khẩn trương cài đặt các bản cập nhật mới nhất của Windows để bảo đảm an toàn, đặc biệt là các bản vá cho 78 lỗ hổng bảo mật đã được Microsoft phát hành, trong đó có 05 lỗ hổng Zero-day đang bị khai thác.

- Các đơn vị cần nâng cao cảnh giác và siết chặt cơ chế quản trị truy cập vào hệ thống ảo hóa, đồng thời đầu tư hệ thống an ninh, bảo mật và đủ nhân sự chuyên trách về an toàn, an ninh mạng để phòng tránh các cuộc tấn công mã hóa, đòi tiền chuộc.

2. Tăng cường cảnh giác với các mối đe dọa:

- Tải về danh sách các tên miền lừa đảo liên quan đến dịch vụ LabHost từ FBI (https://www.ic3.gov/CSA/2025/LabHost_Domains.csv) để nhận diện, chặn truy cập và tăng cường cảnh báo về các mối đe dọa từ LabHost.

- Quản trị viên và người dùng cần nâng cao cảnh giác, cài đặt các chương trình diệt virus (AV) chất lượng, đồng thời kiểm tra kỹ lưỡng trước khi chạy các file thực thi có nguy cơ cao như .exe, .bat, v.v. để phòng tránh mã độc đánh cắp thông tin.

- Đặc biệt chú ý đến việc quản lý tên miền chặt chẽ để tránh các sự cố chuyển hướng trang web như trường hợp của Tiki.

3. Sao lưu và kiểm tra khả năng khôi phục dữ liệu định kỳ: Điều này rất quan trọng để giảm thiểu thiệt hại từ các cuộc tấn công ransomware và các cuộc tấn công vào nền tảng ảo hóa.

4. Phối hợp với cơ quan chức năng:

- Trong quá trình thực hiện nếu có khó khăn, vướng mắc, đề nghị liên hệ 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; báo cáo về Sở Giáo dục và Đào tạo tình hình và kết quả thực hiện.

Sở GDĐT đề nghị Thủ trưởng các đơn vị chỉ đạo thực hiện./.

Nơi nhận:
- Như trên;
- Công an TP (để p/h);
- Lưu: VT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
THÀNH PHỐ HẢI PHÒNG

Uông Minh Long