

Số: /SGDDĐT-QLCL
V/v cảnh báo chiến dịch tấn công mã
độc lợi dụng Đại hội Đảng

Đà Nẵng, ngày tháng 11 năm 2025

Kính gửi:

- Chánh Văn phòng, trưởng các phòng thuộc Sở;
- Các trường, trung tâm trực thuộc Sở.

Ngày 10/11/2025, Sở Giáo dục và Đào tạo (GDĐT) nhận được Công văn số 442/CATP-PA05 của Công an thành phố về việc cảnh báo chiến dịch tấn công mã độc lợi dụng Đại hội Đảng. Nhằm phòng tránh mã độc, đảm bảo an toàn thông tin các hệ thống thông tin cơ quan nhà nước, máy tính người dùng cuối của cán bộ, công chức, viên chức và người lao động. Sở GDĐT thông tin đến các đơn vị, trường học được biết và cách ứng phó mã độc, nội dung cụ thể như sau:

1. Thông tin mã độc

a) Thông tin chung

- **Chủng loại mã độc:** Valley RAT
- **Chức năng:** Mã độc Valley RAT là một loại Remote Access Trojan (RAT) được phát hiện đầu năm 2023, chủ yếu tấn công người dùng dựa qua các chiến dịch phishing (lừa nạt nhân tài tài liệu mỗi nhữ có chứa mã độc). Mục đích của Valley RAT là giám sát và kiểm soát hệ thống bị nhiễm, từ đó tải thêm các plugin độc hại khác để gây hại sâu hơn. Đây là mã độc đa giai đoạn và đa thành phần, có khả năng tránh bị phát hiện bằng cách tải các thành phần theo từng giai đoạn.
- **Phương thức phát tán:** Ngụy trang dưới tệp tin văn bản "DỰ THẢO NGHỊ QUYẾT ĐẠI HỘI.exe". Ngoài ra còn phát tán dưới các tệp tin khác.

b) Thông tin IoC (Indicators of Compromise)

Địa chỉ máy chủ điều khiển (C2): 27.124.9.13, port 5689

2. Biện pháp ứng phó

Các đơn vị, trường học quán triệt đến toàn thể cán bộ, công chức, viên chức và người lao động không truy cập đường dẫn; tải tập tin lạ không rõ nguồn gốc trên không gian mạng; rà quét mã độc trước khi mở tập tin;

Thực hiện rà soát, cập nhật dữ liệu phần mềm bảo mật, phần mềm quét mã độc máy tính tại đơn vị, trường học. Trong trường hợp chưa có phần mềm

phòng chống mã độc tập trung của thành phố thì khuyến nghị cài đặt và sử dụng các phần mềm sau: Avast bản free, AVG bản free, Bitdefender bản free, Windows Defender bản cập nhật mới nhất.

Nhận được Công văn này, Sở GDĐT đề nghị trưởng các phòng thuộc Sở, lãnh đạo các đơn vị, trường học triển khai thực hiện. Mọi trao đổi, hỗ trợ xin liên hệ Công an thành phố (qua Phòng An ninh mạng và Phòng chống tội phạm sử dụng công nghệ cao, Số điện thoại: 0236.3636.010./).

Nơi nhận:

- Như trên;
- CATP;
- Giám đốc, Phó Giám đốc Sở;
- Lưu: VT, QLCL.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Nguyễn Hoàng Nam