

TP. Nam Định, ngày 15 tháng 11 năm 2024

Kính gửi: Hiệu trưởng các trường Mầm non, Tiểu học,
THCS thành phố Nam Định.

Thực hiện công văn số 2104/UBND-NC ngày 14 tháng 11 năm 2024 về việc cảnh báo chiến dịch tấn công mạng có chủ đích vào các hệ thống quan trọng. Thời gian qua, Công an thành phố phát hiện và ghi nhận 03 thông tin liên quan đến các chiến dịch tấn công mạng sử dụng mã độc để thực hiện các hành vi trái phép. Cụ thể:

1. Mallox Ransomware, nổi lên từ năm 2023 hoạt động dưới dạng RAAS (Ransomware as a Service), cho phép các cuộc tấn công trên phạm vi toàn cầu, đặc biệt tại Brazil, Việt Nam và Trung Quốc. Mallox lây nhiễm qua việc khai thác lỗ hổng phần mềm và brute force trên máy chủ MS SQL hoặc PostgreSQL, sau đó triển khai mã độc như Remcos RAT hoặc bộ tải .NET để tải mã độc giai đoạn tiếp theo. Các phiên bản mới đã tối ưu hóa mã hóa bằng AES-256 và ECC, đồng thời tránh mã hóa trên các hệ thống dùng ngôn ngữ của các nước thuộc khối Liên Xô cũ.

2. Chiến dịch tấn công do nhóm Earth Hundun thực hiện trong năm 2024, trong đó sử dụng mã độc RAT để tiến hành các chuỗi tấn công và lan truyền mã độc vào các thiết bị khác. Qua quá trình phân tích, các chuyên gia bảo mật đã phát hiện nhiều chủng mã độc, công cụ độc hại được sử dụng trong chuỗi lây nhiễm như: VenomRAT, Agent-Tesla, Remcos, NjRAT, NanoCore RAT, Pony, Xworm, AsyncRAT và DCRat.

3. Hệ thống giám sát của Viettel Cyber Security ghi nhận tăng đột biến các chiến dịch tấn công ransomware vào hạ tầng ảo hóa của tổ chức, doanh nghiệp tại Việt Nam. Trong đó, các cuộc tấn công ransomware vào hệ thống của VNDIRECT, PVOIL... thời gian vừa qua đã gây gián đoạn hoạt động và thiệt hại về vật chất, hình ảnh của đơn vị cũng như hoạt động bảo đảm an toàn không gian mạng quốc gia.

Để chủ động phòng ngừa các cuộc tấn công sử dụng mã độc RAT, Phòng GDĐT thành phố giao các trường MN, TH, THCS thực hiện một số nội dung sau:

1. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi mã độc trên. Chủ động theo dõi các thông tin liên quan đến mã độc từ hãng nhằm thực hiện nâng cấp lên phiên bản mới nhất để tránh nguy cơ bị tấn công.

2. Tăng cường giám sát và sẵn sàng phương án xử lý khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời thường xuyên theo dõi kênh cảnh

báo của các cơ quan chức năng và các tổ chức lớn về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.

3. Các trường chủ động quản lý hệ thống thông tin tăng cường theo dõi, giám sát, kịp thời phát hiện khi có dấu hiệu xuất hiện các file lạ trên máy tính, tốc độ xử lý của máy tính chậm bất thường ngay lập tức tắt kết nối internet; sử dụng phần mềm quét virus trên máy tính để quét. Trong trường hợp có sự cố nghiêm trọng ở mức độ cao, khẩn cấp hoặc vượt quá khả năng khắc phục của đơn vị phải báo cáo ngay về Phòng GDĐT (qua đồng chí Lê Văn Dũng - SĐT 0918508997) hoặc liên hệ trực tiếp đồng chí Trung tá Nguyễn Hùng Cường - Đội trưởng đội An ninh Công an thành phố, SĐT: 0948.429.966 để xử lý, khắc phục sự cố đảm bảo an toàn, an ninh mạng.

Phòng GDĐT yêu cầu Hiệu trưởng các trường Mầm non, Tiểu học, THCS nghiêm túc triển khai thực hiện./.

Nơi nhận:

- Như trên;
- Lãnh đạo và chuyên viên Phòng GDĐT;
- Lưu VT.



TRƯỞNG PHÒNG

Nguyễn Thế Lâm