UBND TỈNH ĐỒNG NAI **SỞ CÔNG THƯƠNG**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 5060 /SCT-VP V/v triển khai an toàn thông tin mạng, cảnh báo về chiến dịch tấn công có chủ đích vào các hệ thống quan trọng.	*Đồng Nai, ngày 18 tháng 9 năm 2024*

Kính gửi: Các phòng, đơn vị trực thuộc Sở.

Sở Công Thương nhận được các Văn bản của Sở Thông tin và Truyền thông gồm: Văn bản số 3105/STTTT-CĐS ngày 16/9/2024 báo cáo an toàn thông tin mạng Việt Nam (Tháng 8/2024) và Văn bản số 3103/STTTT-CĐS ngày 16/9/2024 về việc cảnh báo về chiến dịch tấn công có chủ đích vào các hệ thống quan trọng.

Thông tin chi tiết về chiến dịch tấn công cụ thể như sau:

- Trong thời gian gần đây, Trung tâm Giám sát an toàn không gian mạng quốc gia ghi nhận các chiến dịch tấn công nhắm vào các tổ chức và doanh nghiệp với mục tiêu chính là tấn công mạng, đánh cắp thông tin và phá hoại hệ thống.

- 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.

- Nhóm APT Lazarus đã phát tán mã độc thông qua phần mềm họp video giả mạo tên FCCCall trong các chiến dịch tấn công chuyên gia blockchain và dự án web game. Lazarus tiếp cận mục tiêu qua các nền tảng tìm kiếm việc làm như LinkedIn và sử dụng Telegram để trích xuất dữ liệu. Mã độc BeaverTail và InvisibleFerret được sử dụng để đánh cắp thông tin từ trình duyệt, ví tiền ảo và ứng dụng quản lý mật khẩu, cũng như cấu hình AnyDesk truy cập từ xa. Mã độc này còn được nhúng vào các dự án Node.js trên GitHub, Gitlab để ẩn mã độc và tránh bị phát hiện.

- Nhóm APT Stately Taurus (Mustang Panda) đã khai thác lỗ hổng trên Visual Studio Code, sử dụng tính năng reverse shell để thực thi mã từ xa và tải xuống payload độc hại. Nhóm sử dụng OpenSSH để chuyển file, quét mạng bằng SharpNBTScan và nén dữ liệu qua Listeners.bat trước khi trích xuất lên Dropbox. Các chuyên gia cũng phát hiện sự tham gia của mã độc ShadowPad, gợi ý khả năng hợp tác giữa hai nhóm tấn công.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Sở, của tỉnh và góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Công Thương đề nghị các đơn vị nghiên cứu, tổ chức triển khai thực hiện các nội dung:

1. Trưởng các phòng, đơn vị tăng cường thực hiện tuyên truyền, quán triệt đến toàn thể công chức, viên chức, người lao động trong cơ quan, đơn vị được biết các thông tin về chiến dịch tấn công có chủ đích vào các hệ thống quan trọng và các nguy cơ rủi ro trong Báo cáo số 14/BC-CATTT ngày 10/9/2024 của Cục An toàn thông tin; tuyên truyền về danh sách các website giả mạo, lừa đảo phát hiện trong tháng (*Phụ lục I trong Báo cáo gửi kèm theo Văn bản số 3105/STTTT-CĐS ngày 16/9/2024*).

2. Sở Công Thương giao Văn phòng Sở và 02 Trung tâm kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi chiến dịch tấn công trên. Chủ động theo dõi các thông tin liên quan đến các chiến dịch tấn công mạng nhằm thực hiện ngăn chặn sớm, tránh nguy cơ bị tấn công mạng.

3. 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.

Trong quá trình thực hiện, nếu có thông tin cần hỗ trợ đề nghị liên hệ với Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin, Bộ Thông tin và Truyền thông, điện thoại: 024.3209.1616 hoặc số điện thoại trực đường dây nóng hỗ trợ giám sát, cảnh báo sớm 0961.405.333, thư điện tử: ncsc@ais.gov.vn hoặc Sở Thông tin và Truyền thông, điện thoại 0251.3810.269, thư điện tử: attt@dongnai.gov.vn./.

Đề nghị các phòng, đơn vị trực thuộc Sở tổ chức triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Ban Giám đốc Sở (báo cáo);
- Lưu: VT, CNTT.

Thuymtt

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ CÔNG THƯƠNG
TỈNH ĐỒNG NAI

Văn Hữu Đồng