UBND TỈNH ĐỒNG NAI
TIỂU BAN AN TOÀN, AN NINH MẠNG

Số: 3811/TBATANM

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

Đồng Nai, ngày 24 tháng 9 năm 2024

V/v Cảnh báo chiến dịch tấn công mạng có chủ đích nhằm tới Việt Nam.

Kính gửi:
- Các Sở, ban, ngành;
- UBND các huyện, thành phố.

Trong thời gian qua, phát hiện chiến dịch tấn công mạng có chủ đích mới sử dụng kỹ thuật AppDomainManager Injection để tán phát mã độc từ tháng 07/2024. Chiến dịch này có thể liên quan đến nhóm APT 41, đã ảnh hưởng đến các tổ chức chính phủ và quân sự trong khu vực Châu Á - Thái Bình Dương trong đó có cả Việt Nam.

Để bảo đảm an toàn hệ thống thông tin, Tiểu ban An toàn, an ninh mạng tỉnh Đồng Nai dề nghị các sở, ban, ngành và địa phương tổ chức kiểm tra, rà soát và xác định các hệ thống, thiết bị có khả năng bị ảnh hưởng bởi chiến dịch tấn công trên để tránh nguy cơ bị tấn công. Đồng thời, tăng cường giám sát, sẵn sàng phương án xử lý, ứng cứu sự cố khi phát hiện có dấu hiệu bị khai thác, tấn công (*kèm phụ lục thông tin chi tiết*).

Trong quá trình thực hiện nếu có khó khăn, vướng mắc đề nghị báo cáo Tiểu ban An toàn, an ninh mạng (qua Công an tỉnh, Sở Thông tin và Truyền thông) để được hướng dẫn.

Tiểu ban An toàn, an ninh mạng tỉnh Đồng Nai thông báo đến các đồng chí nội dung trên để triển khai thực hiện./.

Nơi nhận:
- Như trên;
- Đ/c Võ Tấn Đức - Chủ tịch UBND tỉnh (báo cáo);
- Các đ/c thành viên TBATANM (theo dõi);
- Lưu: VT, PA05.

KT. TRƯỞNG TIỂU BAN
PHÓ TRƯỞNG TIỂU BAN

Đại tá Nguyễn Hồng Phong
Giám đốc Công an tỉnh

Phụ lục

THÔNG TIN VỀ CHIẾN DỊCH TẤN CÔNG CÓ CHỦ ĐÍCH SỬ DỤNG KỸ THUẬT APP DOMAIN MANAGERINJECTION

(Kèm theo Công văn số 3811/PA05-Đ3 ngày 24/9/2024 của PA05)

1. Thông tin chi tiết

Chiến dịch tấn công có chủ đích sử dụng kỹ thuật AppDomainManager Injection để phát tán mã độc kể từ tháng 07/2024. Qua phân tích, mã độc trong chiến dịch này được xác định là CobaltStrike (framework về kiểm thử xâm nhập, cho phép tin tặc tấn công thực thi mã từ xa), với các dấu hiệu kỹ thuật và hạ tầng tương tự nhóm APT41. Chiến dịch đã gây ra những tác động ảnh hưởng đến các tổ chức chính phủ tại Đài Loan, các đơn vị quân sự ở Philippines,... Điều này cho thấy quy mô và tính chất nguy hiểm của cuộc tấn công, đòi hỏi các biện pháp phòng chống nâng cao từ các cơ quan an ninh mạng trong khu vực.

Các đơn vị có thể tải xuống các mã JOC tại địa chỉ https://alert.khonggianmang.vn./

Dưới đây là một so IoC liên quan đến các tấn công gần đây

krislab[.] site	msn-rnicrosoft[.] org
s2cloud-amazon[.] com	s3bucket-azure[.] online
s3cloud-azure[.] com	s3-microsoft[.] com
trendmicrotech[.] com	visualstudio-microsoft[.] com
xtools[.] lol	0

2. Tài liệu tham khảo

https://jp.security.ntt/techs_blog/appdomainmanager-injection