

UBND TỈNH ĐẮK LẮK
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số: /STTTT-CNTT
V/v cảnh báo chiến dịch tấn công mạng có
chủ đích nhằm tới Việt Nam

Đắk Lắk, ngày tháng năm 2024

Kính gửi:

- Các sở, ban, ngành của tỉnh;
- UBND các huyện, thị xã, thành phố.

Thực hiện Công văn số 1720/CATTT-NCSC ngày 26/8/2024 của Cục An toàn thông tin, Bộ Thông tin và Truyền thông về việc cảnh báo chiến dịch tấn công mạng có chủ đích nhằm tới Việt Nam được Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông phát hiện và ghi nhận các thông tin liên quan đến chiến dịch tấn công mạng.

(Thông tin chi tiết xem tại Phụ lục kèm theo)

Nhằm tăng cường công tác an toàn an ninh thông tin, an ninh mạng cho các hệ thống thông tin của các cơ quan, đơn vị, Sở Thông tin và Truyền thông đề nghị các cơ quan, đơn vị triển khai các nội dung như sau:

- 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 chiến dịch nhằm thực hiện ngăn chặn nhằm tránh nguy cơ bị tấn công.
- 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 về an toàn thông tin để phát hiện kịp thời các nguy cơ tấn công mạng.
- Trong trường hợp cần thiết có thể liên hệ đầu mối hỗ trợ của Cục An toàn thông tin: Trung tâm Giám sát an toàn không gian mạng quốc gia, điện thoại 02432091616, thư điện tử: ncsc@ais.gov.vn.

Sở Thông tin và Truyền thông kính đề nghị các cơ quan, đơn vị quan tâm, triển khai các nội dung như trên./.

Nơi nhận:

- Như trên;
- UBND tỉnh (b/c);
- Cục An toàn thông tin (b/c);
- ĐAKLAKIOC(t/h);
- Lưu: VT, CNTT

GIÁM ĐỐC

Trương Hoài Anh

Phụ lục**THÔNG TIN CHI TIẾT VỀ CHIẾN DỊCH TẤN CÔNG**

(Kèm theo Công văn số /STTTT-CNTT ngày /8/2024 của Sở Thông tin và Truyền thông)

1. Thông tin chi tiết

Trung tâm Giám sát an toàn thông tin, Cục An toàn thông tin ghi nhận thông tin liên quan đến chiến dịch tấn công có chủ đích sử dụng kỹ thuật AppDomainManager Injection để phát tán mã độc kể từ tháng 7/2024.

Qua phân tích, mã độc trong chiến dịch này được xác định là CobaltStrike, 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 IOC tại <https://alert.khonggianmang.vn/>

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

krislab[.] site	msn-microsoft[.] 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