ỦY BAN NHÂN DÂN **HUYỆN GIA LÂM**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 2880 /UBND-VHTT V/v cảnh báo chiến dịch tấn công mạng có chủ đích nhắm tới Việt Nam	*Gia Lâm, ngày 04 tháng 9 năm 2024*

Kính gửi:
- Các phòng, ban, đơn vị, trường học thuộc Huyện;
- UBND các xã, thị trấn.

Căn cứ Công văn số 2526/STTTT-ATTTT&GDĐT ngày 29/8/2024 của Sở Thông tin và Truyền thông Hà Nội về việc cảnh báo chiến dịch tấn công mạng có chủ đích nhắm tới Việt Nam. Trong quá trình giám sát an toàn thông tin trên không gian mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), thuộc Cục An toàn thông tin, Bộ Thông tin và Truyền thông, đã phát hiện và ghi nhận một chiến dịch tấn công có chủ đích mới sử dụng kỹ thuật AppDomainManager Injection để phát tán 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, bao gồm cả Việt Nam. *(thông tin chi tiết xem tại Phụ lục kèm theo)*

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của cơ quan, đơn vị góp phần bảo đảm an toàn cho không gian mạng Việt Nam, UBND huyện đề nghị các phòng, ban, đơn vị, trường học thuộc huyện thực hiện nội dung sau:

1. 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.

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. 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.

UBND Huyện yêu cầu các đơn vị triển khai thực hiện./.

Nơi nhận: - Như trên; - Đ/c Trương Văn Học-PCT UBND huyện; - Lưu: VT, VHTT.	**TM. ỦY BAN NHÂN DÂN** **CHỦ TỊCH** **Đặng Thị Huyền**

Phụ lục

THÔNG TIN CHI TIẾT VỀ CHIẾN DỊCH TẤN CÔNG

(Kèm theo Công văn số 2880/UBND-VHTT ngày 04/ 9/2024 của UBND huyện Gia Lâm)

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