SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH THANH HÓA
TRUNG TÂM CNTT&TT

Số: 291 /TTCNTT&TT-QTHT
V/v cảnh báo chiến dịch tấn công mạng có chủ đích nhằm tới Việt Nam

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

Thanh Hoá, ngày 04 tháng 9 năm 2024

Kính gửi:
- Văn phòng Tỉnh ủy;
- Văn phòng Đoàn ĐBQH và HĐND tỉnh;
- Văn phòng UBND tỉnh;
- Các sở, ban, ngành, đơn vị sự nghiệp cấp tỉnh;
- UBND các huyện, thị xã, thành phố;
- Các tổ chức đoàn thể chính trị cấp tỉnh;
- Các doanh nghiệp VT, CNTT trên địa bàn tỉnh.

Căn cứ Công văn số 1720/CATTT-NCSC ngày 26/08/2024 về việc cảnh báo chiến dịch tấn công mạng có chủ đích nhằm tới Việt Nam của Cục An toàn thông tin, Bộ Thông tin và Truyền thông. Theo đó, 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 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)

Để bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin trong các cơ quan nhà nước trên địa bàn tỉnh, Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa đề nghị các cơ quan, đơn vị chỉ đạo các bộ phận, cá nhân thực hiện những nội dung sau:

1. Tổ chức cập nhật các dấu hiệu tấn công trên thiết bị Tường lửa của đơn vị để ngăn chặn các kết nối từ bên trong và ngoài vào danh sách các địa chỉ tên miền độc hại tại Phụ lục kèm theo. Khẩn trương thực hiện kiểm tra, rà soát, xác định máy tính và các hệ thống thông tin trong phạm vi cơ quan, các đơn vị trực thuộc và UBND cấp xã có khả năng bị ảnh hưởng bởi chiến dịch tấn công trên.

2. Tăng cường giám sát và triển khai thực hiện đầy đủ các phương án bảo đảm an toàn thông tin theo Hồ sơ đề xuất cấp độ đã được phê duyệt; 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. Chỉ đạo Tổ ứng cứu sự cố an toàn thông tin mạng tại cơ quan, địa phương mình triển khai chủ động rà soát và sẵn sàng phương án xử lý sự cố khi phát hiện có dấu hiệu bị khai thác, tấn công mạng; đồng thời phổ biến, tuyên truyền kịp thời các nguy cơ về mất an toàn thông tin được cảnh báo của các cơ quan chức năng trong phạm vi cơ quan, địa phương.

Trong quá trình thực hiện, nếu gặp khó khăn, vướng mắc về kỹ thuật liên quan đến các nội dung, công việc trên đề nghị liên hệ với Trung tâm Công nghệ thông tin và Truyền thông Thanh Hóa để phối hợp hỗ trợ, xử lý.

Điện thoại: (0237)3718.699; Thư điện tử: ungcuusuco@thanhhoa.gov.vn./.

Nơi nhận:
- Như kính gửi;
- Sở TT&TT (để b/c);
- PGĐ Sở Nguyễn Văn Tước (để b/c);
- Giám đốc Trung tâm (để b/c);
- Lưu: VT, QTHT.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Trần Ngọc Hưng

Phụ lục
THÔNG TIN CHI TIẾT VỀ CHIẾN DỊCH TẤN CÔNG

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

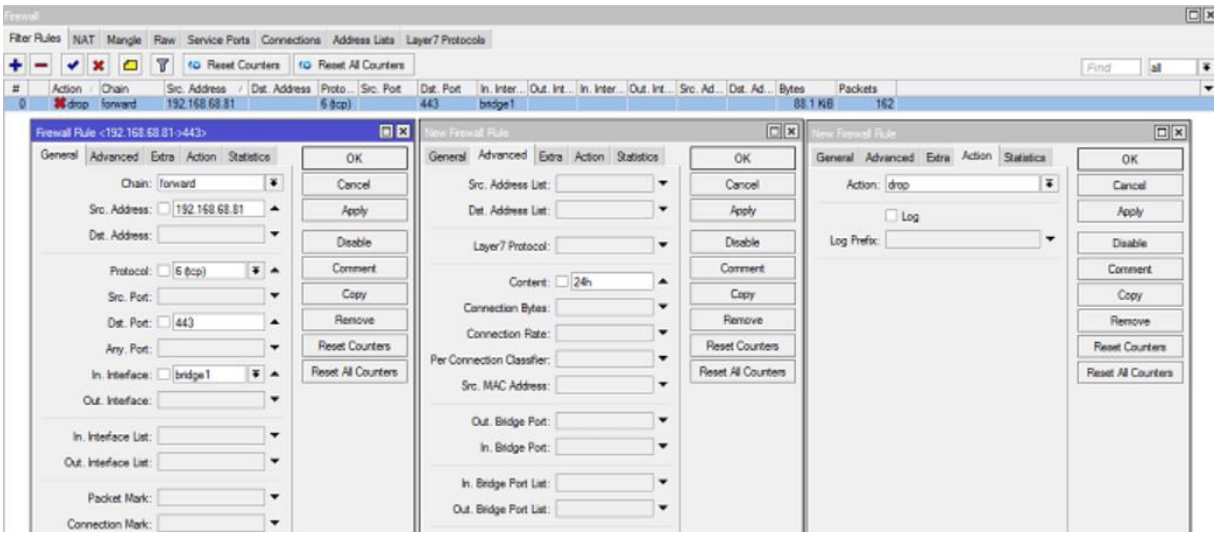
krislab[.] site	msn-microsoft[.] org
s2cloud-amazon[.] com	s3bucket-azure[.] online
s3cloud-azure[.] com	s3-microsoft[.] com
trendmicrotech[.] com	visualstudio-microsoft[.] com
xtools[.] lol	0

2. Hướng dẫn ngăn chặn

Ghi chú: Cách thức thiết lập trên các thiết bị bảo mật sẽ được thực hiện khác nhau, trong bài viết này hướng dẫn trên dòng thiết bị Router Mikrotik có tích hợp chức năng Tường lửa.

2.1. Cập nhật ngăn chặn truy cập vào các tên miền độc hại trên hệ thống thiết bị bảo mật (Tường lửa) tại đơn vị

Trên thiết bị tường lửa (Ví dụ thiết bị Mikrotik) vào IP → Firewall → Filter Rules và thêm một rule mới với nội dung như ảnh dưới:



Trong đó:

- Chain: forward, xử lý các gói tin đi qua router.

- Src. Address: Địa chỉ (hoặc nhóm địa chỉ) IP cần áp dụng rule firewall để ngăn chặn truy cập

- Protocol: Giao thức, chọn 6 (tcp).

- Dst. Port: Port (cổng) cần chặn, ở đây chọn port https 443.

- In. Interface: Interface gói tin đi vào. Chọn bridge, VLAN hoặc interface cụ thể cần chặn.

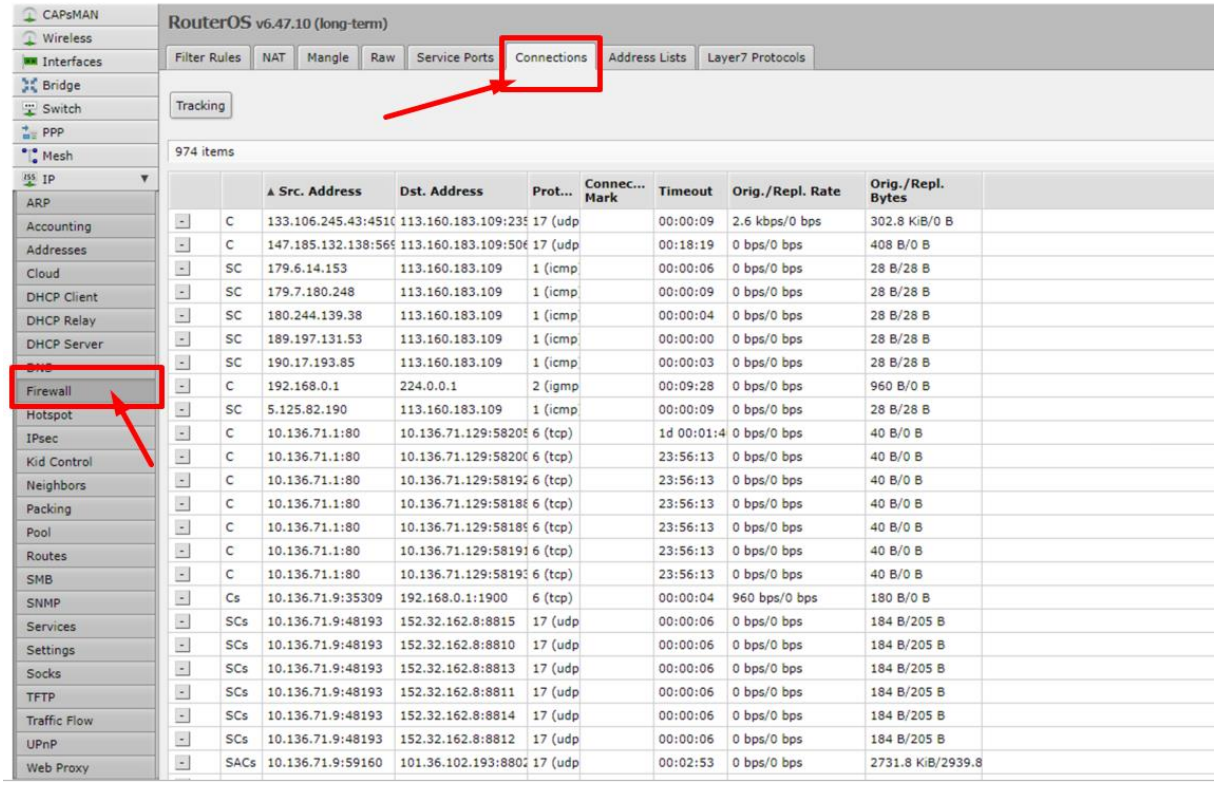
- Content: Nội dung cần chặn.

- Action: Cách xử lý gói tin. Chọn drop (bỏ gói tin đi).

2.2. Theo dõi, rà soát các kết nối trên máy tính tại đơn vị

2.2.1. Theo dõi nhật ký truy cập trên thiết bị bảo mật

Trên thiết bị bảo mật, theo dõi thường xuyên trạng thái kết nối từ các máy tính để ghi nhận tình trạng lây nhiễm của các máy (nếu có).

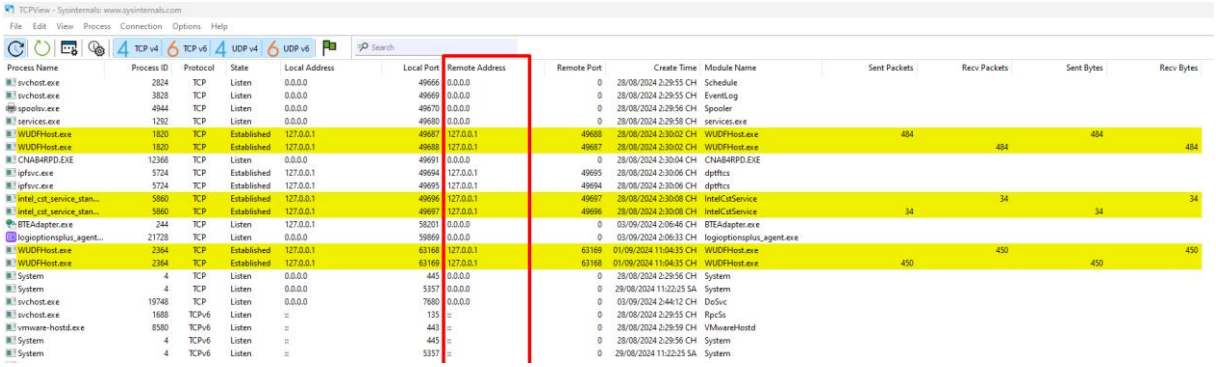


2.2.1. Theo dõi trạng thái kết nối trên các máy tính

Bước 1: Tải công cụ TcpView của hãng Microsoft từ địa chỉ sau:

https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview

Bước 2: Chạy công cụ với quyền quản trị trên máy tính cần kiểm tra. Trên phần Options, chọn chức năng Resolve Addresses để phân giải các địa chỉ IP sang tên miền để theo dõi.



Theo dõi những địa chỉ tên miền tại phần Remote Addresses để ghi nhận xem có địa chỉ nào trong danh sách độc hại mà máy tính đang kết nối đến hay không.