

SỞ THÔNG TIN VÀ TRUYỀN THÔNG CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
TỈNH THANH HÓA
TRUNG TÂM CNTT&TT

Độc lập - Tự do - Hạnh phúc

Số: /TTCNTT&TT-QTHT

Thanh Hoá, ngày tháng năm 2024

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

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: unguusuco@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

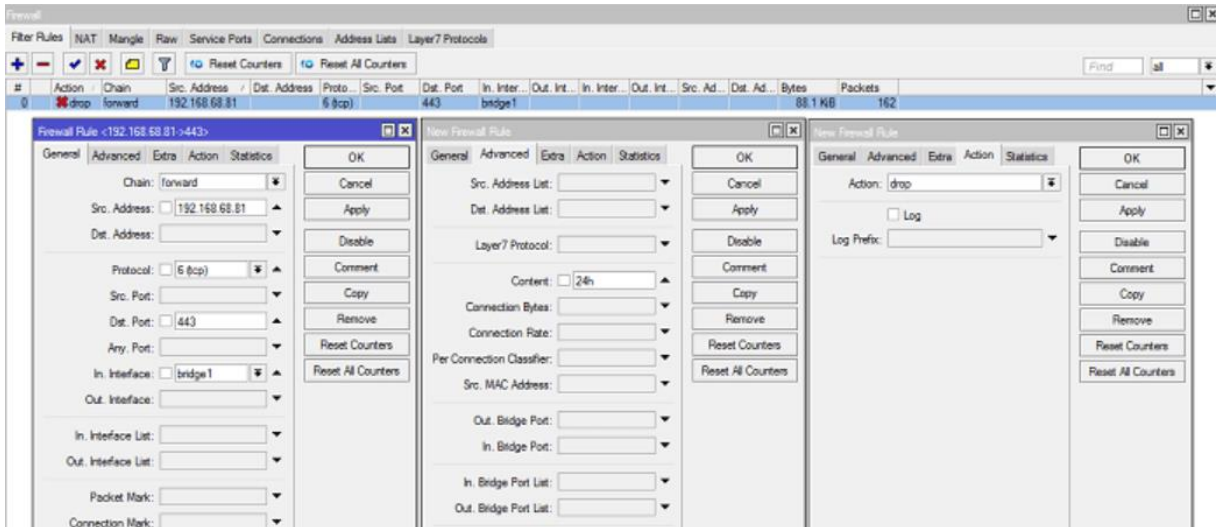
krislab[.] site	msn-microsoft[.] org
s2cloud-amazon[.] com	s3bucket-azure[.] online
s3cloud-azure[.] com	s3-microsoft[.] com
trendmicrotech[.] com	visualstudio-microsoft[.] com
xtools[.] lol	0

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).

RouterOS v6.47.10 (long-term)

Filter Rules NAT Mangle Raw Service Ports **Connections** Address Lists Layer7 Protocols

Tracking

974 items

		Src. Address	Dst. Address	Prot...	Conne... Mark	Timeout	Orig./Repl. Rate	Orig./Repl. Bytes
C		133.106.245.43:4510	113.160.183.109:235	17 (udp)		00:00:09	2.6 kbps/0 bps	302.8 KiB/0 B
C		147.185.132.138:565	113.160.183.109:506	17 (udp)		00:18:19	0 bps/0 bps	408 B/0 B
SC		179.6.14.153	113.160.183.109	1 (icmp)		00:00:06	0 bps/0 bps	28 B/28 B
SC		179.7.180.248	113.160.183.109	1 (icmp)		00:00:09	0 bps/0 bps	28 B/28 B
SC		180.244.139.38	113.160.183.109	1 (icmp)		00:00:04	0 bps/0 bps	28 B/28 B
SC		189.197.131.53	113.160.183.109	1 (icmp)		00:00:00	0 bps/0 bps	28 B/28 B
SC		190.17.193.85	113.160.183.109	1 (icmp)		00:00:03	0 bps/0 bps	28 B/28 B
C		192.168.0.1	224.0.0.1	2 (igmp)		00:09:28	0 bps/0 bps	960 B/0 B
SC		5.125.82.190	113.160.183.109	1 (icmp)		00:00:09	0 bps/0 bps	28 B/28 B
C		10.136.71.1:80	10.136.71.129:58205	6 (tcp)		1d 00:01:4	0 bps/0 bps	40 B/0 B
C		10.136.71.1:80	10.136.71.129:58206	6 (tcp)		23:56:13	0 bps/0 bps	40 B/0 B
C		10.136.71.1:80	10.136.71.129:58192	6 (tcp)		23:56:13	0 bps/0 bps	40 B/0 B
C		10.136.71.1:80	10.136.71.129:58186	6 (tcp)		23:56:13	0 bps/0 bps	40 B/0 B
C		10.136.71.1:80	10.136.71.129:58185	6 (tcp)		23:56:13	0 bps/0 bps	40 B/0 B
C		10.136.71.1:80	10.136.71.129:58193	6 (tcp)		23:56:13	0 bps/0 bps	40 B/0 B
Cs		10.136.71.9:35309	192.168.0.1:1900	6 (tcp)		00:00:04	960 bps/0 bps	180 B/0 B
SCs		10.136.71.9:48193	152.32.162.8:8815	17 (udp)		00:00:06	0 bps/0 bps	184 B/205 B
SCs		10.136.71.9:48193	152.32.162.8:8810	17 (udp)		00:00:06	0 bps/0 bps	184 B/205 B
SCs		10.136.71.9:48193	152.32.162.8:8813	17 (udp)		00:00:06	0 bps/0 bps	184 B/205 B
SCs		10.136.71.9:48193	152.32.162.8:8811	17 (udp)		00:00:06	0 bps/0 bps	184 B/205 B
SCs		10.136.71.9:48193	152.32.162.8:8814	17 (udp)		00:00:06	0 bps/0 bps	184 B/205 B
SCs		10.136.71.9:48193	152.32.162.8:8812	17 (udp)		00:00:06	0 bps/0 bps	184 B/205 B
SACs		10.136.71.9:59160	101.36.102.193:8802	17 (udp)		00:02:53	0 bps/0 bps	2731.8 KiB/2939.8

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.

TCPView - Sysinternals www.sysinternals.com

File Edit View Process Connection Options Help

TCP v4 TCP v6 UDP v4 UDP v6

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets	Recv Packets	Sent Bytes	Recv Bytes
svchost.exe	2824	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	28/08/2024 2:29:55 CH	Schedule				
svchost.exe	3828	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	28/08/2024 2:29:55 CH	EventLog				
spoolsv.exe	4944	TCP	Listen	0.0.0.0	49670	0.0.0.0	0	28/08/2024 2:29:56 CH	Spooler				
services.exe	1292	TCP	Listen	0.0.0.0	49680	0.0.0.0	0	28/08/2024 2:29:58 CH	services.exe				
WUDFHost.exe	1820	TCP	Established	127.0.0.1	49687	127.0.0.1	49688	28/08/2024 2:30:02 CH	WUDFHost.exe	484	484	484	484
WUDFHost.exe	1820	TCP	Established	127.0.0.1	49688	127.0.0.1	49687	28/08/2024 2:30:02 CH	WUDFHost.exe				
CNABRPD.EXE	12368	TCP	Listen	0.0.0.0	49691	0.0.0.0	0	28/08/2024 2:30:04 CH	CNABRPD.EXE				
ipfsvc.exe	5724	TCP	Established	127.0.0.1	49694	127.0.0.1	49695	28/08/2024 2:30:06 CH	ipfthcs				
ipfsvc.exe	5724	TCP	Established	127.0.0.1	49695	127.0.0.1	49694	28/08/2024 2:30:06 CH	ipfthcs				
intel_cst_service_stan...	5860	TCP	Established	127.0.0.1	49696	127.0.0.1	49697	28/08/2024 2:30:08 CH	IntelCstService		34	34	34
intel_cst_service_stan...	5860	TCP	Established	127.0.0.1	49697	127.0.0.1	49696	28/08/2024 2:30:08 CH	IntelCstService	34		34	
BTEAdapter.exe	244	TCP	Listen	127.0.0.1	58201	0.0.0.0	0	03/09/2024 2:56:46 CH	BTEAdapter.exe				
logiptionsplus_agent...	21728	TCP	Listen	0.0.0.0	59869	0.0.0.0	0	03/09/2024 2:56:33 CH	logiptionsplus_agent.exe				
WUDFHost.exe	2364	TCP	Established	127.0.0.1	63168	127.0.0.1	63169	01/09/2024 11:04:25 CH	WUDFHost.exe		450		450
WUDFHost.exe	2364	TCP	Established	127.0.0.1	63169	127.0.0.1	63168	01/09/2024 11:04:25 CH	WUDFHost.exe	450		450	
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	28/08/2024 2:29:56 CH	System				
System	4	TCP	Listen	0.0.0.0	5357	0.0.0.0	0	28/08/2024 11:22:25 SA	System				
svchost.exe	19748	TCP	Listen	0.0.0.0	7680	0.0.0.0	0	03/09/2024 2:44:12 CH	DoSvc				
svchost.exe	1688	TCPv6	Listen	::	135	::	0	28/08/2024 2:29:55 CH	RpcSs				
vmtoolsd-hostid.exe	8930	TCPv6	Listen	::	445	::	0	28/08/2024 2:29:59 CH	VMAwareHostd				
System	4	TCPv6	Listen	::	445	::	0	28/08/2024 2:29:56 CH	System				
System	4	TCPv6	Listen	::	5357	::	0	28/08/2024 11:22:25 SA	System				

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.