BỘ THÔNG TIN TRUYỀN THÔNG
CỤC AN TOÀN THÔNG TIN

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

Số: 2448 /CATTT-NCSC
V/v Cảnh báo chiến dịch tấn công có chủ đích của nhóm APT Earth Estries

Hà Nội, ngày 22 tháng 11 năm 2024

Kính gửi:

- Đơn vị chuyên trách về CNTT/ATTT các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;
- Các Tập đoàn, Tổng công ty nhà nước;
- Các Doanh nghiệp cung cấp dịch vụ viễn thông, Internet và nền tảng số;
- Các Tổ chức tài chính, Ngân hàng thương mại;
- Hệ thống các đơn vị chuyên trách về an toàn thông tin.

Thực hiện chức năng giám sát an toàn thông tin trên không gian mạng, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC), Cục An toàn thông tin, Bộ Thông tin và Truyền thông, đã phát hiện và ghi nhận thông tin liên quan đến chiến dịch tấn công có chủ đích của nhóm APT Earth Estries. Nhóm sử dụng hai chuỗi tấn công có điểm tương đồng với nhau để khai thác lỗ hổng an toàn thông tin tồn tại trên các hệ thống như máy chủ Microsoft Exchange, công cụ quản lý adapter mạng, mục tiêu chủ yếu là các đơn vị quản lý hạ tầng mạng và hệ thống thông tin quan trọng.

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

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của Quý Đơn vị, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Cục An toàn thông tin đề nghị Quý Đơn vị thực hiện:

1. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi lỗ hổng an toàn thông tin trên. Chủ động theo dõi các thông tin liên quan đến đến các chiến dịch tấn công mạng nhằm thực hiện ngăn chặn sớm, 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. Gửi báo cáo kết quả rà soát hệ thống về Cục An toàn thông tin **chậm nhất trước ngày 04/12/2024**. 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.

Trân trọng./.

Nơi nhận:
- Như trên;
- Thứ trưởng Phạm Đức Long (để b/c);
- Cục A05 (Bộ Công an);
- Bộ Tư lệnh 86 (Bộ Quốc phòng);
- Ban Cơ yếu Chính phủ;
- Đơn vị chuyên trách về CNTT/ATTT của: Văn phòng Trung ương Đảng; Văn phòng Quốc hội; Văn phòng Chủ tịch nước; Tòa án nhân dân tối cao; Viện Kiểm sát nhân dân tối cao; Ủy ban Trung ương Mặt trận Tổ quốc Việt Nam;
- Các Cục: Viễn thông, Bưu điện Trung ương;
- Trung tâm VNNIC, Trung tâm Thông tin;
- Ngân hàng Chính sách xã hội;
- Ngân hàng Phát triển Việt Nam;
- Ngân hàng Hợp tác xã Việt Nam;
- Ngân hàng Thương mại Cổ phần;
- Các công ty Cổ phần Chứng khoán;
- Các Tổ chức, doanh nghiệp hoạt động trong lĩnh vực thương mại điện tử;
- Các tổ chức, doanh nghiệp cung cấp dịch vụ trung gian thanh toán, ví điện tử;
- P.ATHTTT, P.QHPT, VNCERT/CC;
- Lưu: VT, NCSC.LTQ.

Q. CỤC TRƯỞNG

CỘNG HÒA X.H.C.N VIỆT NAM
CỤC AN TOÀN THÔNG TIN
BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Trần Quang Hưng

Phụ lục

THÔNG TIN CHI TIẾT VỀ LỖ HỔNG AN TOÀN THÔNG TIN

(Kèm theo Công văn số /CATTT-NCSC ngày / /2024 của Cục An toàn thông tin)

1. Thông tin chi tiết các chiến dịch tấn công

Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin ghi nhận thông tin liên quan chiến dịch tấn công có chủ đích của nhóm APT Earth Estries. Nhóm Earth Estries thực hiện các chiến dịch tấn công tinh vi bằng cách khai thác lỗ hổng trên các hệ thống như Microsoft Exchange và công cụ quản lý adapter mạng. Nhóm sử dụng các mã độc như Cobalt Strike, Crowdoor, Zingdoor, và SnappyBee để lây lan, duy trì kết nối, thu thập dữ liệu và che giấu lưu lượng mạng thông qua proxy nội bộ, đồng thời liên tục cập nhật công cụ để né tránh phát hiện. Các dữ liệu đánh cắp được trích xuất tới các dịch vụ chia sẻ file ẩn danh hoặc máy chủ C&C.

Ngoài các mã độc kể trên, hệ thống mục tiêu còn chứa mã độc Cryptmerlin có chức năng thực thi lệnh gửi tới từ máy chủ C&C và FuxosDoor mã độc cài vào IIS trên máy chủ Exchange, thực thi lệnh sử dụng cmd.exe.

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

Một số IoC liên quan đến các tấn công gần đây:

Mã băm SHA256 của file mã độc

42d4eb7f041116318913 79c5cce55480d2d9d2ef 8feaf1075e1aed0c52df4 bb9	95062728536f23b13357 56ae1a1d68f1df22d585 94ece9998cae6b73772f d49f	6a4de5c7787e212dea5f0 33f8f7cd39aefc93e7c83 c8564dc2204813e8e76ff 2
27042218e8d1a0491525 b35a6dc2fc0737841bca ed65b751e78769eadeda 9751	c32156a7de42a61f5d58 4e82dfbced690d23fd72 080024c14a9143e5f20f 0ad8	a298031b1c28f11f00d3b 9f6311fbfae881d6c789e 70c4bc5e6ccdf8165b94c 6
cdde7878ed0529f9ef3ad 58aa3084f1df6e2fb3718 07b15539187539b060fe d2	6f274955b1fb58cc9a60 476bc5a9cd9d54c962cc 29e73db41b7786148cb7 4505	09abc579097b0bd8d115 702bb1eeb546d2401373 c83385a52386ad4243f9 45e8
292f70bff5717608c289f 4146febcc06a2c5d8192 529a8c51e18ec0f7b44d 1cf	cd8630f8e07e16203195 f563457a84beb08112fc bb4d9ee1056a788174cf 8f6b	98ddf03ca6ade4770cc06 ac8034b3468bd94094f5 813d28b74885e5ca6958 895

03365cce37db511fdfaf8d77a14f806a2d822a111aa8cc032b5b341c0b0064a5	1378bde3aee0057ca2a5854fee4d184479491ec624a3bbf215098afaa6b82299	b17660d1a4c0258739024187497be0b11530791d1307d9e5556f04f0ac58d42f
b450311b5fc4333b26955f7c709ca61fcfdba168f1a8839a93979a892a8c22cc	39f1c7095e1db05944eeda08a2e1c1b8c513ea581bfc0cb36ad106e3a8f38b5f	0c8c0b2837fbb9c15da1bfb904ed3f3903e2d4d49c999394068f274b014a09dd
a113c637bb81f9bbd39731672b242a8da5915ef4b5e93d72cc9a7454b5e120bd	4aeaa0d954268d4fc7179ec7578258c3459ee95b82698363e0cafb700c05181a	d0575b3ced944dc627d047c60f23d25bd3aa0c4deab69f784b9a80aae50fbd7b
25b9fdef3061c7dfea744830774ca0e289dba7c14be85f0d4695d382763b409b	6d64643c044fe534dbb2c1158409138fcded757e550c6f79eada15e69a7865bc	0

Địa chỉ máy chủ C&C

103.159.133[.]209	45.192.178[.]208	38.54.71[.]140 (Snappybee)
103.159.133[.]205	103.103.131[.]40	103.15.28[.]228
154.220.3[.]17	156.255.2[.]202	103.103.128[.]121
162.19.135[.]182	cdglobalclouds[.]com	broadmediacloud[.]com
zmail.broadmediacloud[.]com (CrowDoor)	www.nodtecloud[.]com	mail2-0da8aa1c.oxcdntech[.]com (Zingdoor)
helpdesk.athenatechlabs[.]com (CrowDoor)	supports.flarecastdns[.]com (CrowDoor)	ns.starkaero[.]com (Cobeacon)
pay.johannesburghotel[.]net (CRYPTMERLIN)	kidshomeworkabc.global.ssl.fastly[.]net (Cobeacon)	ap.missmichiko[.]com (Zingdoor)
portal[.]sppokemon[.]com (Zingdoor)	svn.truecdnnetwork[.]com (Cobeacon)	lync.realtxholdem[.]com
globalnetzone.b-cdn[.]net	amazoncdns[.]com	www[.]euphemismscase[.]site
www[.]dbacloudsupport[.]com	www[.]cloudshappen[.]com	www[.]amazoncdns[.]com
supports[.]dbacloudsupport[.]com	ssl3[.]awsdns-531[.]com	soffice[.]offices-analytics[.]com
services[.]offices-analytics[.]com	resource[.]offices-analytics[.]com	redsquare[.]redcrossco[.]com
portal[.]techmersion[.]com	portal[.]cdglobalclouds[.]com	opengl[.]cloudshappen[.]com

ns108[.]cloudshappen[.]com	ns101[.]awsdns-531[.]com	ms119[.]newsfreecloud[.]com
ms101[.]cloudshappen[.]com	mail[.]euphemismscase[.]site	llnw-dd[.]awsdns-531[.]com
images[.]dbacloudsupport[.]com	helpdesk[.]cloudshappen[.]com	helpdesk[.]athenatechlabs[.]com
global[.]techmersion[.]com	ge[.]huseinhbz[.]click	ftp[.]techmersion[.]com
euphemismscase[.]site	emv1[.]techmersion[.]com	emv1[.]cdglobalclouds[.]com
de[.]huseinhbz[.]click	credits[.]offices-analytics[.]com	cloudsrv[.]cloudfrontsrv[.]com
cdn181[.]awsdns-531[.]com	cdn101[.]cloudflaresrv[.]com	cdglobalclouds[.]com
cas04[.]awsdns-531[.]com	cachecloud[.]cloudflaresrv[.]com	cache10[.]newsfreecloud[.]com
c11r[.]awsdns-531[.]com	blog[.]techmersion[.]com	auth[.]boxlibraries[.]com

2. Tài liệu tham khảo

https://www.trendmicro.com/en_us/research/24/k/breaking-down-earth-estries-persistent-ttps-in-prolonged-cyber-o.html