

Số: /STTTT-BCVT&CNTT Quảng Ngãi, ngày tháng 11 năm 2024

V/v cảnh báo chiến dịch tấn công có chủ đích của nhóm APT Earth Estries

Kính gửi:

- Văn phòng: Tỉnh ủy, Đoàn ĐBQH&HĐND, UBND tỉnh;
- Các sở, ban, ngành; Hội, đoàn thể tỉnh;
- UBND các huyện, thị xã, thành phố;
- Báo Quảng Ngãi, Đài Phát thanh và Truyền hình tỉnh;
- Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Công an tỉnh;
- UBND các xã, phường, thị trấn.

Theo cảnh báo của Cục An toàn thông tin tại Công văn số 2448/CATTT-NCSC ngày 22/11/2024 về việc Cảnh báo chiến dịch tấn công có chủ đích của nhóm APT Earth Estries, Sở Thông tin và Truyền thông đề nghị lãnh đạo các cơ quan, đơn vị chỉ đạo thực hiện một số biện pháp sau để hạn chế các rủi ro về nguy cơ mất an toàn thông tin, cụ thể:

1. Kiểm tra, rà soát hệ thống thông tin đang sử dụng có khả năng bị ảnh hưởng bởi chiến dịch tấn công APT Earth Estries. 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.

3. Gửi báo cáo kết quả rà soát hệ thống về Sở Thông tin và Truyền thông **chậm nhất trước ngày 02/12/2024** để tổng hợp báo cáo Cục An toàn thông tin. Khi phát hiện các hệ thống có biểu hiện bị khai thác, tấn công mạng, triển khai ngay các biện pháp xử lý ngăn chặn tấn công trên hệ thống và thông báo về Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi để có các biện pháp hỗ trợ, xử lý kịp thời.

(Gửi kèm Phụ lục thông tin về Chiến dịch tấn công APT Earth Estries)

Đề nghị lãnh đạo các cơ quan, đơn vị quan tâm chỉ đạo thực hiện./.

Nơi nhận:

- Như trên;
- UBND tỉnh (báo cáo);
- Cục An toàn thông tin (báo cáo);
- Phòng VH&TT các huyện, thị xã, thành phố;
- Thành viên Đội ứng cứu sự cố ATTT mạng tỉnh;
- Sở TT&TT: Lãnh đạo Sở, các phòng chuyên môn, TT CDS;
- Lưu: VT, BCVT&CNTT.

**KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Nguyễn Quốc Huy Hoàng

PHỤ LỤC
THÔNG TIN CHI TIẾT VỀ CHIẾN DỊCH TẤN CÔNG
(Kèm theo Công văn số /STTTT-BCVT&CNTT ngày /11/2024
của Sở Thông tin và Truyền thông)

1. Thông tin chi tiết về chiến dịch tấn công của nhóm APT “Mustang Panda”

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

42d4eb7f04111631891379c5cce55480d2d9d2ef8feaf1075e1aed0c52df4bb9	95062728536f23b1335756ae1a1d68f1df22d58594ece9998cae6b73772fd49f	6a4de5c7787e212dea5f033f8f7cd39aefc93e7c83c8564dc2204813e8e76ff2
27042218e8d1a0491525b35a6dc2fc0737841bcaed65b751e78769eaded9751	c32156a7de42a61f5d584e82dfbced690d23fd72080024c14a9143e5f20f0ad8	a298031b1c28f11f00d3b9f6311fbfae881d6c789e70c4bc5e6ccdf8165b94c6
cdde7878ed0529f9ef3ad58aa3084f1df6e2fb371807b15539187539b060fed2	6f274955b1fb58cc9a60476bc5a9cd9d54c962cc29e73db41b7786148cb74505	09abc579097b0bd8d115702bb1eeb546d2401373c83385a52386ad4243f945e8
292f70bff5717608c289f4146febcc06a2c5d8192529a8c51e18ec0f7b44d1cf	cd8630f8e07e16203195f563457a84beb08112fcb4d9ee1056a788174cf8f6b	98ddf03ca6ade4770cc06ac8034b3468bd94094f5813d28b74885e5ca695889
03365cce37db511fdfaf8d77a14f806a2d822a111aa8cc032b5b341c0b0064a5	1378bde3aee0057ca2a5854fee4d184479491ec624a3bbf215098afaa6b82299	b17660d1a4c0258739024187497be0b11530791d1307d9e5556f04f0ac58d42f
b450311b5fc4333b26955f7c709ca61fcfdb168f1a8	39f1c7095e1db05944eeda08a2e1c1b8c513ea581bfc	0c8c0b2837fbb9c15da1fbb904ed3f3903e2d4d49c99

839a93979a892a8c22cc	0cb36ad106e3a8f38b5f	9394068f274b014a09dd
a113c637bb81f9bbd3973 1672b242a8da5915ef4b5e 93d72cc9a7454b5e120bd	4aeaa0d954268d4fc7179e c7578258c3459ee95b826 98363e0cafb700c05181a	d0575b3ced944dc627d04 7c60f23d25bd3aa0c4deab 69f784b9a80aae50fbd7b
25b9fdef3061c7dfea7448 30774ca0e289dba7c14be 85f0d4695d382763b409b	6d64643c044fe534dbb2c 1158409138fcded757e55 0c6f79eada15e69a7865bc	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[.]c om (Zingdoor)
helpdesk.athenatechlabs[.] com (CrowDoor)	supports.flarecastdns[.]com (CrowDoor)	ns.starkaero[.]com (Cobeacon)
pay.johannesburghotel[.] net (CRYPTMERLIN)	kidshomeworkabc.global.ssl.f astly[.]net (Cobeacon)	ap.missmichiko[.]com (Zingdoor)
portal[.]sppokemon[.]co m (Zingdoor)	svn.truecdnnetwork[.]com (Cobeacon)	lync.realtxholdem[.]co m
globalnetzone.b- cdn[.]net	amazoncdns[.]com	www[.]euphemismscas e[.]site
www[.]dbacloudsupport[.] com	www[.]cloudshappen[.]com	www[.]amazoncdns[.]c om
supports[.]dbacloudsupp ort[.]com	ssl3[.]awsdns-531[.]com	soffice[.]offices- analytics[.]com
services[.]offices- analytics[.]com	resource[.]offices- analytics[.]com	redsquare[.]redcrossco[.] com
portal[.]techmersion[.]co m	portal[.]cdglobalclouds[.]com	opengl[.]cloudshappen[.] com
ns108[.]cloudshappen[.]c om	ns101[.]awsdns-531[.]com	ms119[.]newsfreecloud[.] com
ms101[.]cloudshappen[.] com	mail[.]euphemismscase[.]site	l1nw-dd[.]awsdns- 531[.]com
images[.]dbacloudsuppor t[.]com	helpdesk[.]cloudshappen[.]co m	helpdesk[.]athenatechla bs[.]com
global[.]techmersion[.]co m	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
