UBND TỈNH KIÊN GIANG
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

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

Số :701 /STTTT-CĐS
V/v rà soát dấu hiệu của các chiến dịch tấn công có chủ đích (APT)

Kiên Giang, ngày 01 *tháng 04 năm 2024*

Kính gửi:
- Văn phòng Tỉnh ủy;
- Văn phòng UBND tỉnh;
- Sở, ban, ngành cấp tỉnh;
- UBND các huyện, thành phố;
- Phòng Văn hóa - Thông tin các huyện, thành phố.

Sở Thông tin và Truyền thông Kiên Giang nhận được Công văn số 424/CATTT-NCSC ngày 22/03/2024 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông về việc rà soát dấu hiệu của các chiến dịch tấn công có chủ đích (APT).

Theo Công văn số 424/CATTT-NCSC ngày 22/03/2024, trong quá trình giám sát an toàn thông tin trên không gian mạng, Cục An toàn thông tin ghi nhận các chiến dịch tấn công có chủ đích (APT) có khả năng ảnh hưởng đến nhiều cơ quan, tổ chức tại Việt Nam.

Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin của các cơ quan nhà nước trên địa bàn tỉnh, góp phần bảo đảm an toàn cho không gian mạng Việt Nam, Sở Thông tin và Truyền thông Kiên Giang đề nghị các đơn vị chủ động thực hiện các biện pháp sau:

1. Rà soát toàn bộ hệ thống thông tin thuộc phạm vi quản lý của mình đồng thời cập nhật các giải pháp bảo mật để phát hiện và xử lý kịp thời các dấu hiệu tấn công *(Thông tin kỹ thuật để thực hiện rà soát tại Phụ lục kèm theo).*

2. Kiểm tra, rà soát dữ liệu lưu trữ trên các hệ thống phòng chống mã độc tập trung, hệ thống giám sát an toàn thông tin (SOC) từ tháng 01/2023 đến nay để phát hiện các dấu hiệu, sự kiện, cảnh báo liên quan đến các tấn công có chủ đích *(Thông tin kỹ thuật để thực hiện rà soát tại Phụ lục kèm theo)*.

3. Báo cáo kết quả rà soát gửi về Phòng Chuyển đổi số - Sở Thông tin và Truyền thông trước 17/04/2024 để tổng hợp báo cáo hoặc ngay khi phát hiện dấu hiệu tấn công liên hệ theo đầu mối sau:

- Trung tâm Giám sát an toàn không gian mạng quốc gia: Ông Nguyễn Văn Chung, Trưởng phòng Giám sát An toàn thông tin, Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC); Điện thoại: 0345551337; Thư điện tử: chungnv@ais.gov.vn.

- Hoặc Phòng Chuyển đổi số - Sở Thông tin và Truyền thông Kiên Giang, điện thoại: 0297.3921678, 0918767498 (đ/c Nghỉ), thư điện tử: ttnghi.stttt@kiengiang.gov.vn.

Trân trọng./.

Nơi nhận:
- Như trên;
- Trung tâm CNTT&TT (thực hiện);
- Lưu: VT, CĐS (ttnghi).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XHCN VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH KIÊN GIANG

Nguyễn Xuân Kiệm

PHỤ LỤC

THÔNG TIN KỸ THUẬT PHỤC VỤ RÀ SOÁT

(Kèm theo Công văn số 701 /STTTT-CĐS ngày 01/ 04 /2024 của Sở Thông tin và Truyền Thông Kiên Giang)

1. Địa chỉ IP/Tên miền độc hại

TT	Địa chỉ IP/Domain	TT	Địa chỉ IP/Domain
1	23[.]106[.]122[.]5	28	getfilefox[.]com
2	207[.]148[.]69[.]1	29	ivibers[.]com
3	45[.]76[.]157[.]92	30	meetviberapi[.]com
4	50[.]7[.]61[.]26	31	iamc2c2[.]com
5	50[.]7[.]61[.]27	32	thisistestc2[.]com
6	50[.]7[.]61[.]28	33	electrictulsa[.]com
7	207[.]148[.]75[.]122	34	mongolianshipregistrar[.]com
8	45[.]32[.]33[.]17	35	103.107.104[.]37
9	23[.]106[.]122[.]46	36	149.104.12[.]64
10	23[.]106[.]124[.]152	37	185.82.216[.]184
11	115[.]126[.]98[.]204	38	195.211.96[.]99
12	118[.]99[.]6[.]202	39	195.123.246[.]26
13	199[.]231[.]211[.]19	40	149.104.12[.]64
14	www[.]security-microsoft[.]net	41	45.83.236[.]105
15	update[.]centos-yum[.]com	42	45.131.179[.]179
16	update[.]microsoft-setting[.]com	43	103.192.226[.]46
17	update[.]windows[.]server-microsoft[.]com	44	154[.]204.27.181
18	149[.]28[.]26[.]2	45	103[.]56.53.120
19	cdn-dev[.]helpkaspersky[.]top	46	176[.]113.69.91
20	data-dev[.]helpkaspersky[.]top	47	45.251.240[.]55
21	happy[.]gitweb[.]cloudns[.]nz	48	149.104.11[.]29
22	support[.]helpkaspersky[.]top	49	web.bonuscave[.]com
23	gtldgtld[.]store	50	www.markplay[.]net
24	softupdate[.]xyz	51	images.markplay[.]net

25	tfirstdaily[.]store	52	news.comsnews[.]com
26	estmongolia[.]com	53	images.kiidcloud[.]com
27	getfiledown[.]com		

2. Mã băm của mẫu mã độc sử dụng trong các chiến dịch

10b2a7c9329b232e4eef81bac6ba26323e3683ac1f8a99d3a9f8965da5036b6f
18f4f14857e9b7e3aa1f6f21f21396abd5f421342b7f4d00402a4aff5a538fa1
1e278cfe8098f3badedd5e497f36753d46d96d81edd1c5bee4fc7bc6380c26b3
244c32c4809a5ea72dfd2a53d0c535f17ba3b33e4c3ee6ed229858d687a2563a
35f16e469047cf4ef78f87a616d26ec09e3d6a3d7a51415ea34805549a41dcfa
3f0aa01ed70bc2ab29557521a65476ec2ff2c867315067cc8a5937d63bcbe815
50cdd2397836d33a8dc285ed421d9b7cc69e38ba0421638235206fd466299dab
57f64f170dfeaa1150493ed3f63ea6f1df3ca71ad1722e12ac0f77744fb1a829
5a32bf21904387d469d4f8cdaff46048e99666fc9b4d74872af9379df7979bfe
6fd7697efc137faf2d3ad5d63ffe4743db70f905a71dbed76207beeeb04732f2
898a7527c065454ba9fad0e36469e12b214f5a3bd40a5ec7fcaf9b75afc34dce
c14f6ac5bcd8645eb80a612a6bf6d58c31b0e28e50be871f278c341ed1fa8c7c
d17fe5bc3042baf219e81cbbf991749dfcd8b6d73cf6506a8228e19910da3578
d31d135bc450eafa698e6b7fb5d11b4926948163af09122ca1c568284d8b33b3
e0f109836a025d4531ea895cebecc9bdefb84a0cc747861986c4bc231e1d4213
e42466863837a655b814d2fb6aa2381369b8c5a9fe100e512085617f775dac36
ee41eb21f439b1168ae815ca067ee91d84d6947397d71e214edc6868dbf4f272
2e3645c8441f2be4182869db5ae320da00c513e0cb643142c70a833f529f28aa
8218c23361e9f1b25ee1a93796ef471ca8ca5ac672b7db69ad05f42eb90b0b8d
2e850cb2a1d06d2665601cefd88802ff99905de8bc4ea348ea051d4886e780ee
521b3add2ab6cee5a5cfd53b78e08ef2214946393d2a156c674606528b05763a
9ada058a558b7cadb238fc2c259f204369cd604e927f9712fd51262ca6987cb1
9d4e18ae979bdf6b57e685896b350b23c428d911eee14af133c3ee7d208f8a82
bb4e7b0c969895fc9836640b80e2bdc6572d214ba2ee55b77588f8a4eedea5a4
d176951b9ff3239b659ad57b729edb0845785e418852ecfeef1669f4c6fed61b
fe4fad660bb44e108ab07d812f8b1bbf16852c1b881a5e721a9f811cae317f39
01b09cb97a58ea0f9bf2b98b38b83f0cfc9f97f39f7bfd73a990c9b00bcdb66c
05b63707ca3cad54085e521aee84c7472ff7b3fe05e22fd65c8e2ee6f36c6243
241737842eb17676b3603e2f076336b7bc6304accef3057401264affb963bef8
5a6a0e01949799dc72c030b4ad8149446624dcd9645ba3eefda981c3fda26472
b4c470be7e434dac0b61919a6b0c5b10cf7a01a22c5403c4540afdb5f2c79fab
c377b79732e93f981998817e6f0e8664578b474445ba11b402c70b4b0357caab
f66a6b49a23cf3cc842a84d955c0292e7d1c0718ec4e78d4513e18b6c53a94ac
acfcf97ee4ff5cc7f5ecdc6f92ea132e29c48400ab6244de64f9b9de4368deb2
ccd4a648cc2c4a5bbcd148f9c182f4c9595440a41dd3ea289a11609063c86a6d
ea140cc8da39014c1454c3f6a036d5f43aa26c215cb9981ab2b7076f2388b73e
ffef75582ad185c58135cf02e347c0ad6d46751fcfbb803dc3e70b73729e6136
4b653253049a65142f827706203de55f03abccbcddac3ed2171d79bf8186eda9
63b7d8c4c740c54ab91db94dd89b2c8313ecb7ba13524c646fdb10facf5c470d
6d03c6b7621990f84580eaa094393fbf896803c86779644506b115692b70bd64

f6993e767306d4cbf676bf3c4a56fc2ad1d5cb6c4f67563f6de2f28b79f2b934
992d3df19c453a84b5b46c5742fb22686c65eb48cfc71b0bbc7e94c0ef13e66e
bb6afc28d610bfddcd0cf3497c152c081f63137fea9914a1fd461a0706c74288
15412d1a6b7f79fad45bcd32cf82f9d651d9ccca082f98a0cca3ad5335284e45
6302acdfce30cec5e9167ff7905800a6220c7dda495c0aae1f4594c7263a29b2
98b5b4f96d4e1a9a6e170a4b2740ce1a1dfc411ada238e42a5954e66559a5541
a2c3073fa5587f8a70d7def7fd8355e1f6d20eb906c3cd4df8c744826cb81d91
bf830191215e0c8db207ea320d8e795990cf6b3e6698932e6e0c9c0588fc9eff
ebdf3d3e0867b29e66d8b7570be4e6619c64fae7e1fbd052be387f736c980c8e
1d3d460b22f70cc26252673e12dfd85da988f69046d6b94602576270df590b2c
36acdaceb9abfcf9923378c44037cc5df8aac03406d082d552e96462121c4ac1
46b84d55c394c1c504c0fad8b5240bc0a183f5eda03e35d4f7f816bf48bff3e2
4cb020a66fdbc99b0bce2ae24d5684685e2b1e9219fbdfda56b3aace4e8d5f66
67ad30c3359b377d1964a5add97d2dc96b855940685131b302d5ba2c907ef355
6c006620062b40b22d00e7e73a93e6a7fa66ce720093b44b4a0f3ef809fa2716
804387e43fdd1bd45b35e65d52d86882d64956b0a286e8721da402062f95a9e3
82f7bcda95fcc0e690159a2fbd7b3e38ef3ff9105496498f86d1fa9ff4312846
b8f2da1eefa09077d86a443ad688080b98672f171918c06e2b3652df783be03a
da1c9cb862b0be89819a94335eea8bf5ab56e08a1f4ca0ef92fe8d46fd2b1577
f5b6c0d73c513c3c8efbcc967d7f6865559e90d59fb78b2b15394f22fd7315cb
07e38ba00a0477367e63646bbd6e09053ab67939a9c70f062b12b42a2cde82fb
1c0853a5f86bb7eca48a36f07094188adb1a8893cd13309f91f669ba7c8ed124
2e012ba20ecb553745f7719bd477778ba75e324bfec44d03a27a010dac7a2780
2e9da6d50f8b73a00310f91cf1fc79e4804265a08028dcb6272623440bb47497
2f3d89e8db70e7560868c4cf7f03aafa4cd703a13d1d6f814028469806cb6bd7
363f5d92a2692898ed7d5d2caa5e8f51f4db466d0b9134328aafad359e027544
3a3db15bd60f30293cfdf1ca7e159b8040d380665cc0857aed098b471be77030
45e70dbed32cb723ea901c97d0c5682fe0e07e64485095c3e5bbccc86059384e
4aadf0aa60ffd932230c3e88437097a3ba85a2e5587c9b9d92c1ec172f795944
5b17bc2a89727700f94570b0dddc12b315db34dbbd79186177167abbb173cee5
5e1839fed3562d559166f7f9d3e388cdd21da83b67ccb70fa4121825b91469d6
6a4e32229e5ca41e8eca99cefe5beef3e3621c2199f8844b4d218c14b5481534
7102d6b76a4170203daa939072bba548960db436f85113cd1fca0bb554d95b3c
767694e220e5119425ed808bc0801a007022614812868e60962660863de42fa5
799214f6bf40056a1f0c903d5ac59e6216c49a5cd55e5c1a36a0f2c5637e345a
7e5b05d29c3aa2aa178c3cc0338ba52b39dc89dafadeec7301f187db0b060372
7e86d717a13d4c6ccce80098200331d5b963201ce0ffb59dadedbb555bf97d4c
a36d64da109b47022591909362c3f9899efe5f0d8b902460e272761e2b75c75e
a4f59d4d42e42b882068cacf8b70f314add963e2cbbf7a52e70df130bfe23dff
b3a6dfc196bdad381c18f9f861f8da3757479cec2a76b8e5908da5aaec072dd8
d2cc1135c314f526f88fbe19f25d94899d52de7e3422f334437f32388d040d71
d462f3909c3e4b1a13b2fce4843a20f4622a256cd878d3345b3091e61f9ec1fc
dd469fbf68f6bf71e495b3e497e31d17aa1d0af918a943f8637dd3304f840740
ef4a2cfe4d9d3495d4957a65299f608f7b823fab0699fded728fd3900c0b2bb4
fff2f40e74ad7052ec9eeb08fb4aba2d807c3862beed80579944ed85456af1ab
42fecaaf47ed5606d4e4885ce821702a83bbaa4602a13ab0e9b933a04e373956
44b0479dd2debc68480c4cd4759466bf1aac8d3405b99071a61854cb63500448
d310f5baa1c39ada9f60b85ed134b7cd99a04d9a8869f24ec9f3bd28ce9de519

0ff80e4db32d1d45a0c2afdfd7a1be961c0fbd9d43613a22a989f9024cc1b1e9
4529f3751102e7c0a6ec05c6a987d0cc5edc08f75f287dd6ac189abbd1282014
484578b6e7e427a151c309bdc00c90b1c0faf25a8581cace55e2c25ec34056e0
b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682
d096c3a67634599bc47151f0e01a7423a3eb873377371b2b928c0d4f57635a1f
7af402f4bd2b1a2d2d8b74fb7599860f3a90b7b6f66a519f2b4d31aeea2500aa
b19a46f99b649dc731ed5c8410bda7e0385d15e1b9aab1e467b05dccd7753865
bc422a4e1b6a351ac6fe73d496015cfa6a9dbd5e38566c6f44a59faff83ee95a
f34bd1d485de437fe18360d1e850c3fd64415e49d691e610711d8d232071a0b1
f4ea99dc41cb7922d01955eef9303ec3a24b88c3318138855346de1e830ed09e
c9d5dc956841e000bfd8762e2f0b48b66c79b79500e894b4efa7fb9ba17e4e9e
a99bf162a8588b2f318c9460aef78851bd64e4826c2cb124984d2ab357a6beea
0f0663fc26b18212485149e3e22c3dd4b8900ea8dca7c084dbe09fef02cfdade
b153e10c95bb8bfa6dbf5835067c5b45840f057a38ef9b8871b6dc40edcf601f
c2bb47ac533d1413c829a1453b2b854b95aabebf1b26b446bd1ad0838f1e09de
c7ec098093eb08d2b36d1c37b928d716d8da021f93319a093808a7ceb3b35dc1
25967270d67253c72532a7e0416eb27ff249bc17dc1d7cded0148f8f4b932789
32609faef0b04f0c37c4cf081c147872a45c59d7c4fbca35deb40d144b0226ad
364f38b48565814b576f482c1e0eb4c8d58effcd033fd45136ee00640a2b5321
471e61015ff18349f4bf357447597a5457983933618 8d98d299b14cff458d132
42663f9d1ad0fe190912800b92c64d38b6f74fac23281b87180a4fef5bc2efd6
7c741c8bcd19990140f3fa4aa95bb195929c9429fc47f95cf4ab9fad03040f7b
c9da5b0a8dee27fbf5d7bbb4c9b9b38d8c0c547479d315efd62599a3c5d9cb13
6e625bbcecc45b6b556141eef37ffd31aa4861ce4debca6500be72364172ffc7
dca394742205750041 59ecff70054bcf6239803fcf8d30f4e2e3907b5b97129c
26b1d37ea3da6a6213b65b000dbb39575d858fa274aea895cc3bf62e706fce5d
651c096cf7043a01d939dff9ba58e4d69f15b2244c71b43bedb4ada8c37e8859
f8c1a4c3060bc139d8ac9ad88d2632d40a96a87d58aba7862f35a396a18f42e5
67c23db357588489031700ea8c7dc502a6081d7d1a620c03b82a8f281aa6bde6
b6f375d8e75c438d63c8be429ab3b6608f1adcd233c0cc939082a6d7371c09bb
88c8eb7d2a64e0f675cb2ac3da69cdf314a08a702a65c992bcb7f6d9ec15704b
12c584a685d9dffbee767d7ad867d5f3793518fb7d96ab11e3636edcc490e1bd
71bba2753da5006015bc890d30b1ed207a446e9f34c7e0157d6591bf573f3787
908ff3a80ef065ab4be1942e0d41583903f6aac02d97df6b4a92a07a633397a8
5700535f19a382c8b84db6bff3a077e15269df0ec10ea6257e2fa203720356b4
a5cd617434e8d0e8ae25b961830113cba7308c2f1ff274f09247de8ed74cac4f
0df7e56610adad2ed5adfdfab07faedc08a61d9f944a5448aa62e071cffc28c4
095855cf6c82ae662cce34294f0969ca8c9df266736105c0297d2913a9237dd1
8e4a4d202d57c79dc0f40ae032f9d7b0ea7ce5024128a2aa227decc228e16113
95205b92d597489b33854e70d86f16d46201803a1a9cb5379c0d6b7c0784dbc7
70fac63465187ae5c2f057efc291bc34987dff46bec565a7e8f07f9899527224
8615cc8487833522ffd014c0f0661b3d1bed7a4cb51138b1ee172173002192be
b6e88396594070a92cbf1c313858392b052703944162de64ce3ad494996bd177
583941ca6e1a2e007f5f0e2e112054e44b18687894ac173d0e93e035cea25e83
e3bae2e2b757a76db92ab017328d1459b181f8d98e04b691b62ff65d1e1be280
60b3a42b96b98868cae2c8f87d6ed74a57a64b284917e8e0f6c248c691d51797
eb9e557fac3dd50cc46a544975235ebfce6b592e90437d967c9afba234a33f13
16b62c9dc6060a19a5b64491b7242ace1c707dbe531b843c854fcc1dc39febbe

5dd7813fa8aad22bd6c80811c8c7300f114a8e7897a2bd46343a06884d774914
3fa7eaa4697cfcf71d0bd5aa9d2dbec495d7eac43bdfcfbef07a306635e4973b
a0c94205ca2ed1bcdf065c7aeb96a0c99f33495e7bbfd2ccba36daebd829a916
17225c9e46f809556616d9e09d29fd7c13ca90d25ae21e00cc9ad7857ee66b82
d0ca6917c042e417da5996efa49afca6cb15f09e3b0b41cbc94aab65a409e9dc
d64afd9799d8de3f39a4ce99584fa67a615a667945532cfa3f702adbe27724c4
c4627a5525a7f39205412a915fd52b93d83ef0115ee1b2642705fe1a08320692
39f8288ef21f5d6135f8418a36b9045c9758c4e7a4e4cab4aff4c1c6119f901a
42c18766b5492c5f0eaa935cf88e57d12ffd30d6f3cc2e9e0a3c0bdcdfa44ad5
9610cbcd4561368b6612cad1693982c43c8d81b0d52bb264c5f606f2478c1c58
4c1b5283f05322edfb0ef8b9d5cf75b62b558fcaefed921f1143765a3bd6248e
e6bc87e3e3d98a0a8db4fcd7cd5a9b89d4a7b125de450dfb8f387d2a9e09face
13c31dbbae53517a17f7e6c99031480babe2bd8a07151dbb7f344ab620f3ac11
ca1ada6770b85771f98e5c02310449ab73231034cfa78b8861850368208c7698
abd6521990e88bd18bbcba063744efe0ccac23063bb340720cc3f610d9b1c770
77a49637bf4047959419c41867437957619d03059b5d3f8d9af26e6ae2347db6
f4f36c78cbf9901f224de427f42b390c83190c7c1cc4bce8b66f596e62df02d0
48e37bb7e1ac185d314f262894014e1337a3c14455cd987dd83ac220bae87b3a
33ff6318a3e745420c884f35709f2799f2fe461a6a5bb5b1e3166b9ab2ff142f
04679defa1a4009bddab2a5d81be747b51a7f0f7aa5e7ebb937b40379a6a4690
a102626700691e57ece83a4ce24d995e57449508238eb5688954b78448be9172
1a8aeee97a31f2de076b8ea5c04471480aefd5d82c57eab280443c7c376f8d5c
a0a3eeb6973f12fe61e6e90fe5fe8e406a8e00b31b1511a0dfe9a88109d0d129
cd60e1c7d418a9c6ad4705d315f8ace2cdc3fd0528e71064dd80bbbd51bc2b76
74f3101e869cedb3fc6608baa21f91290bb3db41c4260efe86f9aeb7279f18a1