Mar 19 2024

NETMANAGEIT

Intelligence Report

Earth Krahang Exploits Intergovernmental Trust to Launch Cross-Government Attacks

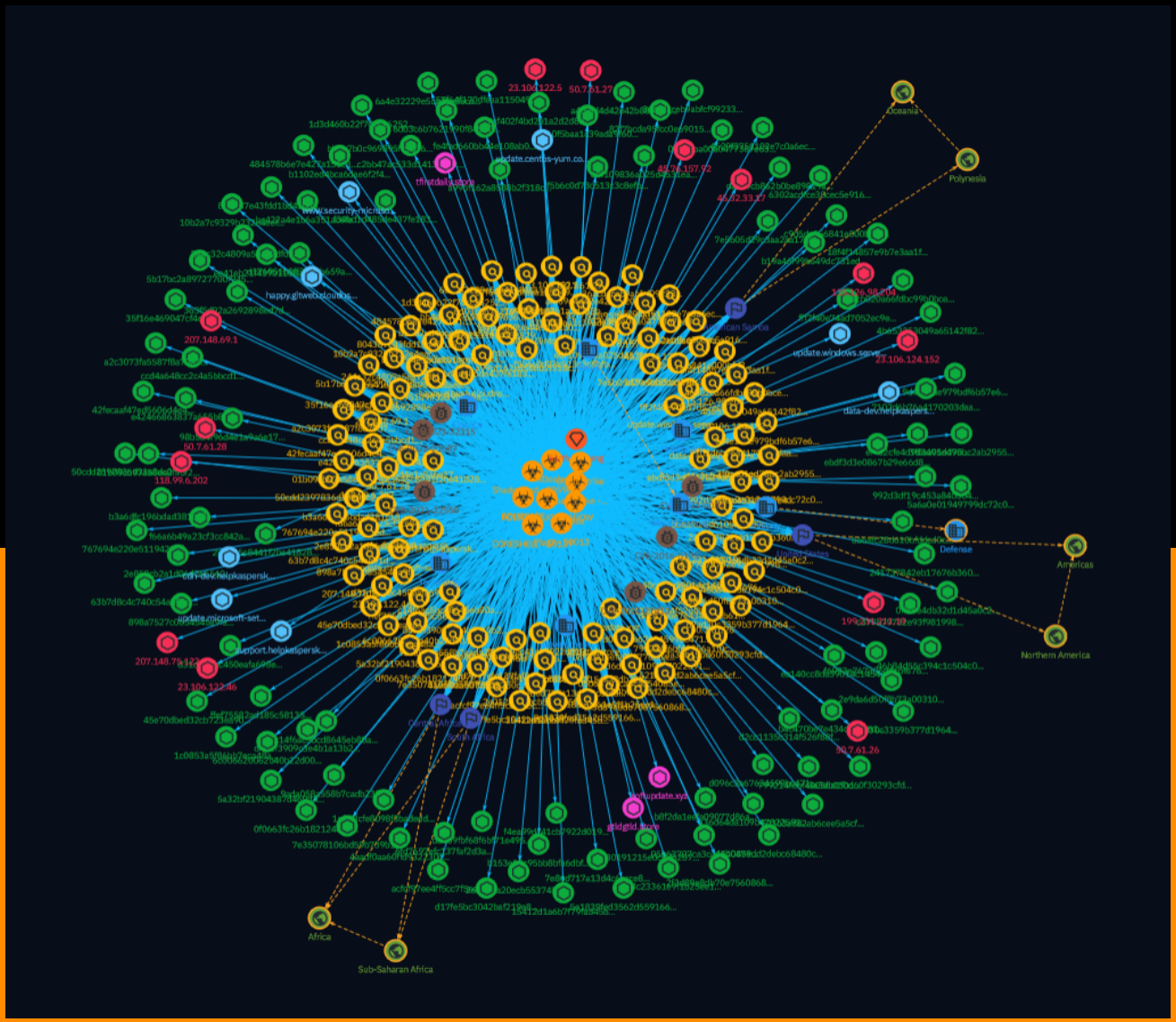

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A threat actor named Earth Krahang has been targeting government entities worldwide since early 2022, focusing on Southeast Asia but also Europe, America, and Africa. The group exploits public-facing servers and sends spear phishing emails to deliver backdoors. Earth Krahang abuses compromised government infrastructure to attack other governments, hosting payloads, proxying traffic, and sending emails. The actor's goal appears to be cyberespionage. Earth Krahang uses the RESHELL and XDealer malware families and post-exploitation tools like Cobalt Strike.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Indicator

Name
www.security-microsoft.net
Pattern Type
stix
Pattern
[hostname:value = 'www.security-microsoft.net']
Name
update.windows.server-microsoft.com
Pattern Type
stix
Pattern
[hostname:value = 'update.windows.server-microsoft.com']
Name
update.microsoft-setting.com

Pattern Type
stix
Pattern
[hostname:value = 'update.microsoft-setting.com']
Name
update.centos-yum.com
Pattern Type
stix
Pattern
[hostname:value = 'update.centos-yum.com']
Name
support.helpkaspersky.top
Pattern Type
stix
Pattern
[hostname:value = 'support.helpkaspersky.top']
Name
happy.gitweb.cloudns.nz

Pattern Type
stix
Pattern
[hostname:value = 'happy.gitweb.cloudns.nz']
Name
data-dev.helpkaspersky.top
Pattern Type
stix
Pattern
[hostname:value = 'data-dev.helpkaspersky.top']
Name
cdn-dev.helpkaspersky.top
Pattern Type
stix
Pattern
[hostname:value = 'cdn-dev.helpkaspersky.top']
Name
tfirstdaily.store

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '12 months ago', 'timestamp': 1680240708, 'iso': '2023-03-31T01:31:48-04:00'} - **IPQS: Domain:** tfirstdaily.store - **IPQS: IP Address:** 149.28.148.26

Pattern Type

stix

Pattern

[domain-name:value = 'tfirstdaily.store']

Name

softupdate.xyz

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** softupdate.xyz - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'softupdate.xyz']

Name

fff2f40e74ad7052ec9eeb08fb4aba2d807c3862beed80579944ed85456af1ab

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fff2f40e74ad7052ec9eeb08fb4aba2d807c3862beed80579944ed85456af1ab']

Name

ffef75582ad185c58135cf02e347c0ad6d46751fcfbb803dc3e70b73729e6136

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ffef75582ad185c58135cf02e347c0ad6d46751fcfbb803dc3e70b73729e6136']

Name

fe4fad660bb44e108ab07d812f8b1bbf16852c1b881a5e721a9f811cae317f39

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fe4fad660bb44e108ab07d812f8b1bbf16852c1b881a5e721a9f811cae317f39']

Name

f6993e767306d4cbf676bf3c4a56fc2ad1d5cb6c4f67563f6de2f28b79f2b934

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f6993e767306d4cbf676bf3c4a56fc2ad1d5cb6c4f67563f6de2f28b79f2b934']

Name

f66a6b49a23cf3cc842a84d955c0292e7d1c0718ec4e78d4513e18b6c53a94ac

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f66a6b49a23cf3cc842a84d955c0292e7d1c0718ec4e78d4513e18b6c53a94ac']

Name

f5b6c0d73c513c3c8efbcc967d7f6865559e90d59fb78b2b15394f22fd7315cb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f5b6c0d73c513c3c8efbcc967d7f6865559e90d59fb78b2b15394f22fd7315cb']

Name

f4ea99dc41cb7922d01955eef9303ec3a24b88c3318138855346de1e830ed09e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f4ea99dc41cb7922d01955eef9303ec3a24b88c3318138855346de1e830ed09e']

Name

f34bd1d485de437fe18360d1e850c3fd64415e49d691e610711d8d232071a0b1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f34bd1d485de437fe18360d1e850c3fd64415e49d691e610711d8d232071a0b1']

Name

ef4a2cfe4d9d3495d4957a65299f608f7b823fab0699fded728fd3900c0b2bb4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ef4a2cfe4d9d3495d4957a65299f608f7b823fab0699fded728fd3900c0b2bb4']

Name

ebdf3d3e0867b29e66d8b7570be4e6619c64fae7e1fbd052be387f736c980c8e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ebdf3d3e0867b29e66d8b7570be4e6619c64fae7e1fbd052be387f736c980c8e']

Name

ee41eb21f439b1168ae815ca067ee91d84d6947397d71e214edc6868dbf4f272

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ee41eb21f439b1168ae815ca067ee91d84d6947397d71e214edc6868dbf4f272']

Name

ea140cc8da39014c1454c3f6a036d5f43aa26c215cb9981ab2b7076f2388b73e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ea140cc8da39014c1454c3f6a036d5f43aa26c215cb9981ab2b7076f2388b73e']

Name

e42466863837a655b814d2fb6aa2381369b8c5a9fe100e512085617f775dac36

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e42466863837a655b814d2fb6aa2381369b8c5a9fe100e512085617f775dac36']

Name

e0f109836a025d4531ea895cebecc9bdefb84a0cc747861986c4bc231e1d4213

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e0f109836a025d4531ea895cebecc9bdefb84a0cc747861986c4bc231e1d4213']

Name

dd469fbf68f6bf71e495b3e497e31d17aa1d0af918a943f8637dd3304f840740

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dd469fbf68f6bf71e495b3e497e31d17aa1d0af918a943f8637dd3304f840740']

Name

d462f3909c3e4b1a13b2fce4843a20f4622a256cd878d3345b3091e61f9ec1fc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd462f3909c3e4b1a13b2fce4843a20f4622a256cd878d3345b3091e61f9ec1fc']

Name

da1c9cb862b0be89819a94335eea8bf5ab56e08a1f4ca0ef92fe8d46fd2b1577

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'da1c9cb862b0be89819a94335eea8bf5ab56e08a1f4ca0ef92fe8d46fd2b1577']

Name

d31d135bc450eafa698e6b7fb5d11b4926948163af09122ca1c568284d8b33b3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd31d135bc450eafa698e6b7fb5d11b4926948163af09122ca1c568284d8b33b3']

Name

d310f5baa1c39ada9f60b85ed134b7cd99a04d9a8869f24ec9f3bd28ce9de519

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd310f5baa1c39ada9f60b85ed134b7cd99a04d9a8869f24ec9f3bd28ce9de519']

Name

d2cc1135c314f526f88fbe19f25d94899d52de7e3422f334437f32388d040d71

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd2cc1135c314f526f88fbe19f25d94899d52de7e3422f334437f32388d040d71']

Name

d176951b9ff3239b659ad57b729edb0845785e418852ecfeef1669f4c6fed61b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd176951b9ff3239b659ad57b729edb0845785e418852ecfeef1669f4c6fed61b']

Name

c9d5dc956841e000bfd8762e2f0b48b66c79b79500e894b4efa7fb9ba17e4e9e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c9d5dc956841e000bfd8762e2f0b48b66c79b79500e894b4efa7fb9ba17e4e9e']

Name

d096c3a67634599bc47151f0e01a7423a3eb873377371b2b928c0d4f57635a1f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd096c3a67634599bc47151f0e01a7423a3eb873377371b2b928c0d4f57635a1f']

Name

ccd4a648cc2c4a5bbcd148f9c182f4c9595440a41dd3ea289a11609063c86a6d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ccd4a648cc2c4a5bbcd148f9c182f4c9595440a41dd3ea289a11609063c86a6d']

Name

c377b79732e93f981998817e6f0e8664578b474445ba11b402c70b4b0357caab

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c377b79732e93f981998817e6f0e8664578b474445ba11b402c70b4b0357caab']

Name

c14f6ac5bcd8645eb80a612a6bf6d58c31b0e28e50be871f278c341ed1fa8c7c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c14f6ac5bcd8645eb80a612a6bf6d58c31b0e28e50be871f278c341ed1fa8c7c']

Name

c2bb47ac533d1413c829a1453b2b854b95aabebf1b26b446bd1ad0838f1e09de

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c2bb47ac533d1413c829a1453b2b854b95aabebf1b26b446bd1ad0838f1e09de']

Name

bf830191215e0c8db207ea320d8e795990cf6b3e6698932e6e0c9c0588fc9eff

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bf830191215e0c8db207ea320d8e795990cf6b3e6698932e6e0c9c0588fc9eff']

Name

bc422a4e1b6a351ac6fe73d496015cfa6a9dbd5e38566c6f44a59faff83ee95a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bc422a4e1b6a351ac6fe73d496015cfa6a9dbd5e38566c6f44a59faff83ee95a']

Name

bb6afc28d610bfddcd0cf3497c152c081f63137fea9914a1fd461a0706c74288

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bb6afc28d610bfddcd0cf3497c152c081f63137fea9914a1fd461a0706c74288']

Name

b8f2da1eefa09077d86a443ad688080b98672f171918c06e2b3652df783be03a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b8f2da1eefa09077d86a443ad688080b98672f171918c06e2b3652df783be03a']

Name

bb4e7b0c969895fc9836640b80e2bdc6572d214ba2ee55b77588f8a4eedea5a4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bb4e7b0c969895fc9836640b80e2bdc6572d214ba2ee55b77588f8a4eedea5a4']

Name

b4c470be7e434dac0b61919a6b0c5b10cf7a01a22c5403c4540afdb5f2c79fab

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b4c470be7e434dac0b61919a6b0c5b10cf7a01a22c5403c4540afdb5f2c79fab']

Name

b3a6dfc196bdad381c18f9f861f8da3757479cec2a76b8e5908da5aaec072dd8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b3a6dfc196bdad381c18f9f861f8da3757479cec2a76b8e5908da5aaec072dd8']

Name

b19a46f99b649dc731ed5c8410bda7e0385d15e1b9aab1e467b05dccd7753865

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b19a46f99b649dc731ed5c8410bda7e0385d15e1b9aab1e467b05dccd7753865']

Name

b153e10c95bb8bfa6dbf5835067c5b45840f057a38ef9b8871b6dc40edcf601f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b153e10c95bb8bfa6dbf5835067c5b45840f057a38ef9b8871b6dc40edcf601f']

Name

b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682']

Name

a99bf162a8588b2f318c9460aef78851bd64e4826c2cb124984d2ab357a6beea

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a99bf162a8588b2f318c9460aef78851bd64e4826c2cb124984d2ab357a6beea']

Name

acfcf97ee4ff5cc7f5ecdc6f92ea132e29c48400ab6244de64f9b9de4368deb2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'acfcf97ee4ff5cc7f5ecdc6f92ea132e29c48400ab6244de64f9b9de4368deb2']

Name

a4f59d4d42e42b882068cacf8b70f314add963e2cbbf7a52e70df130bfe23dff

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a4f59d4d42e42b882068cacf8b70f314add963e2cbbf7a52e70df130bfe23dff']

Name

a36d64da109b47022591909362c3f9899efe5f0d8b902460e272761e2b75c75e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a36d64da109b47022591909362c3f9899efe5f0d8b902460e272761e2b75c75e']

Name

a2c3073fa5587f8a70d7def7fd8355e1f6d20eb906c3cd4df8c744826cb81d91

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a2c3073fa5587f8a70d7def7fd8355e1f6d20eb906c3cd4df8c744826cb81d91']

Name

9d4e18ae979bdf6b57e685896b350b23c428d911eee14af133c3ee7d208f8a82

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9d4e18ae979bdf6b57e685896b350b23c428d911eee14af133c3ee7d208f8a82']

Name

9ada058a558b7cadb238fc2c259f204369cd604e927f9712fd51262ca6987cb1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9ada058a558b7cadb238fc2c259f204369cd604e927f9712fd51262ca6987cb1']

Name

98b5b4f96d4e1a9a6e170a4b2740ce1a1dfc411ada238e42a5954e66559a5541

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '98b5b4f96d4e1a9a6e170a4b2740ce1a1dfc411ada238e42a5954e66559a5541']

Name

992d3df19c453a84b5b46c5742fb22686c65eb48cfc71b0bbc7e94c0ef13e66e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '992d3df19c453a84b5b46c5742fb22686c65eb48cfc71b0bbc7e94c0ef13e66e']

Name

898a7527c065454ba9fad0e36469e12b214f5a3bd40a5ec7fcaf9b75afc34dce

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '898a7527c065454ba9fad0e36469e12b214f5a3bd40a5ec7fcaf9b75afc34dce']

Name

82f7bcda95fcc0e690159a2fbd7b3e38ef3ff9105496498f86d1fa9ff4312846

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '82f7bcda95fcc0e690159a2fbd7b3e38ef3ff9105496498f86d1fa9ff4312846']

Name

8218c23361e9f1b25ee1a93796ef471ca8ca5ac672b7db69ad05f42eb90b0b8d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8218c23361e9f1b25ee1a93796ef471ca8ca5ac672b7db69ad05f42eb90b0b8d']

Name

804387e43fdd1bd45b35e65d52d86882d64956b0a286e8721da402062f95a9e3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '804387e43fdd1bd45b35e65d52d86882d64956b0a286e8721da402062f95a9e3']

Name

7e5b05d29c3aa2aa178c3cc0338ba52b39dc89dafadeec7301f187db0b060372

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7e5b05d29c3aa2aa178c3cc0338ba52b39dc89dafadeec7301f187db0b060372']

Name

7e86d717a13d4c6ccce80098200331d5b963201ce0ffb59dadedbb555bf97d4c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7e86d717a13d4c6ccce80098200331d5b963201ce0ffb59dadedbb555bf97d4c']

Name

7af402f4bd2b1a2d2d8b74fb7599860f3a90b7b6f66a519f2b4d31aeea2500aa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7af402f4bd2b1a2d2d8b74fb7599860f3a90b7b6f66a519f2b4d31aeea2500aa']

Name

799214f6bf40056a1f0c903d5ac59e6216c49a5cd55e5c1a36a0f2c5637e345a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '799214f6bf40056a1f0c903d5ac59e6216c49a5cd55e5c1a36a0f2c5637e345a']

Name

767694e220e5119425ed808bc0801a0070226148128 68e60962660863de42fa5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '767694e220e5119425ed808bc0801a0070226148128 68e60962660863de42fa5']

Name

7102d6b76a4170203daa939072bba548960db436f85113cd1fca0bb554d95b3c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7102d6b76a4170203daa939072bba548960db436f85113cd1fca0bb554d95b3c']

Name

6fd7697efc137faf2d3ad5d63ffe4743db70f905a71dbed76207beeeb04732f2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6fd7697efc137faf2d3ad5d63ffe4743db70f905a71dbed76207beeeb04732f2']

Name

6d03c6b7621990f84580eaa094393fbf896803c86779644506b115692b70bd64

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6d03c6b7621990f84580eaa094393fbf896803c86779644506b115692b70bd64']

Name

gtldgtld.store

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '11 months ago', 'timestamp': 1681284971, 'iso': '2023-04-12T03:36:11-04:00'} - **IPQS: Domain:** gtldgtld.store - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'gtldgtld.store']

Name

6c006620062b40b22d00e7e73a93e6a7fa66ce720093b44b4a0f3ef809fa2716

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6c006620062b40b22d00e7e73a93e6a7fa66ce720093b44b4a0f3ef809fa2716']

Name

6a4e32229e5ca41e8eca99cefe5beef3e3621c2199f8844b4d218c14b5481534

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6a4e32229e5ca41e8eca99cefe5beef3e3621c2199f8844b4d218c14b5481534']

Name

67ad30c3359b377d1964a5add97d2dc96b855940685131b302d5ba2c907ef355

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '67ad30c3359b377d1964a5add97d2dc96b855940685131b302d5ba2c907ef355']

Name

63b7d8c4c740c54ab91db94dd89b2c8313ecb7ba13524c646fdb10facf5c470d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '63b7d8c4c740c54ab91db94dd89b2c8313ecb7ba13524c646fdb10facf5c470d']

Name

6302acdfce30cec5e9167ff7905800a6220c7dda495c0aae1f4594c7263a29b2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6302acdfce30cec5e9167ff7905800a6220c7dda495c0aae1f4594c7263a29b2']

Name

5e1839fed3562d559166f7f9d3e388cdd21da83b67ccb70fa4121825b91469d6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5e1839fed3562d559166f7f9d3e388cdd21da83b67ccb70fa4121825b91469d6']

Name

5b17bc2a89727700f94570b0dddc12b315db34dbbd79186177167abbb173cee5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5b17bc2a89727700f94570b0dddc12b315db34dbbd79186177167abbb173cee5']

Name

5a6a0e01949799dc72c030b4ad8149446624dcd9645ba3eefda981c3fda26472

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5a6a0e01949799dc72c030b4ad8149446624dcd9645ba3eefda981c3fda26472']

Name

5a32bf21904387d469d4f8cdaff46048e99666fc9b4d74872af9379df7979bfe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5a32bf21904387d469d4f8cdaff46048e99666fc9b4d74872af9379df7979bfe']

Name

57f64f170dfeaa1150493ed3f63ea6f1df3ca71ad1722e12ac0f77744fb1a829

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '57f64f170dfeaa1150493ed3f63ea6f1df3ca71ad1722e12ac0f77744fb1a829']

Name

521b3add2ab6cee5a5cfd53b78e08ef2214946393d2a156c674606528b05763a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '521b3add2ab6cee5a5cfd53b78e08ef2214946393d2a156c674606528b05763a']

Name

50cdd2397836d33a8dc285ed421d9b7cc69e38ba0421638235206fd466299dab

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '50cdd2397836d33a8dc285ed421d9b7cc69e38ba0421638235206fd466299dab']

Name

4b653253049a65142f827706203de55f03abccbcddac3ed2171d79bf8186eda9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4b653253049a65142f827706203de55f03abccbcddac3ed2171d79bf8186eda9']

Name

4aadf0aa60ffd932230c3e88437097a3ba85a2e5587c9b9d92c1ec172f795944

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4aadf0aa60ffd932230c3e88437097a3ba85a2e5587c9b9d92c1ec172f795944']

Name

484578b6e7e427a151c309bdc00c90b1c0faf25a8581cace55e2c25ec34056e0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '484578b6e7e427a151c309bdc00c90b1c0faf25a8581cace55e2c25ec34056e0']

Name

46b84d55c394c1c504c0fad8b5240bc0a183f5eda03e35d4f7f816bf48bff3e2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '46b84d55c394c1c504c0fad8b5240bc0a183f5eda03e35d4f7f816bf48bff3e2']

Name

45e70dbed32cb723ea901c97d0c5682fe0e07e64485095c3e5bbccc86059384e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '45e70dbed32cb723ea901c97d0c5682fe0e07e64485095c3e5bbccc86059384e']

Name

4529f3751102e7c0a6ec05c6a987d0cc5edc08f75f287dd6ac189abbd1282014

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4529f3751102e7c0a6ec05c6a987d0cc5edc08f75f287dd6ac189abbd1282014']

Name

44b0479dd2debc68480c4cd4759466bf1aac8d3405b99071a61854cb63500448

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '44b0479dd2debc68480c4cd4759466bf1aac8d3405b99071a61854cb63500448']

Name

42fecaaf47ed5606d4e4885ce821702a83bbaa4602a13ab0e9b933a04e373956

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '42fecaaf47ed5606d4e4885ce821702a83bbaa4602a13ab0e9b933a04e373956']

Name

3f0aa01ed70bc2ab29557521a65476ec2ff2c867315067cc8a5937d63bcbe815

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3f0aa01ed70bc2ab29557521a65476ec2ff2c867315067cc8a5937d63bcbe815']

Name

50.7.61.28

Description

- **Zip Code:** N/A - **ISP:** Fdcservers - **ASN:** 30058 - **Organization:** Fdcservers - **Is Crawler:** False - **Timezone:** Asia/Tokyo - **Mobile:** False - **Host:** 50.7.61.28 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** JP - **Region:** Tokyo - **City:** Tokyo - **Latitude:** 35.62 - **Longitude:** 139.74

Pattern Type

stix

Pattern

[ipv4-addr:value = '50.7.61.28']

Name

36acdaceb9abfcf9923378c44037cc5df8aac03406d082d552e96462121c4ac1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '36acdaceb9abfcf9923378c44037cc5df8aac03406d082d552e96462121c4ac1']

Name

3a3db15bd60f30293cfdf1ca7e159b8040d380665cc0857aed098b471be77030

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3a3db15bd60f30293cfdf1ca7e159b8040d380665cc0857aed098b471be77030']

Name

363f5d92a2692898ed7d5d2caa5e8f51f4db466d0b9134328aafad359e027544

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '363f5d92a2692898ed7d5d2caa5e8f51f4db466d0b9134328aafad359e027544']

Name

45.76.157.92

Description

- **Zip Code:** N/A - **ISP:** Vultr - **ASN:** 20473 - **Organization:** Vultr - **Is Crawler:** False - **Timezone:** Asia/Singapore - **Mobile:** False - **Host:** 45.76.157.92.vultrusercontent.com - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False -

Connection Type: Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** SG - **Region:** Singapore - **City:** Singapore - **Latitude:** 1.31 - **Longitude:** 103.68

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.76.157.92']

Name

2f3d89e8db70e7560868c4cf7f03aafa4cd703a13d1d6f814028469806cb6bd7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2f3d89e8db70e7560868c4cf7f03aafa4cd703a13d1d6f814028469806cb6bd7']

Name

35f16e469047cf4ef78f87a616d26ec09e3d6a3d7a51415ea34805549a41dcfa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '35f16e469047cf4ef78f87a616d26ec09e3d6a3d7a51415ea34805549a41dcfa']

Name

2e9da6d50f8b73a00310f91cf1fc79e4804265a08028dcb6272623440bb47497

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2e9da6d50f8b73a00310f91cf1fc79e4804265a08028dcb6272623440bb47497']

Name

2e850cb2a1d06d2665601cefd88802ff99905de8bc4ea348ea051d4886e780ee

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2e850cb2a1d06d2665601cefd88802ff99905de8bc4ea348ea051d4886e780ee']

Name

2e3645c8441f2be4182869db5ae320da00c513e0cb643142c70a833f529f28aa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2e3645c8441f2be4182869db5ae320da00c513e0cb643142c70a833f529f28aa']

Name

2e012ba20ecb553745f7719bd477778ba75e324bfec44d03a27a010dac7a2780

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2e012ba20ecb553745f7719bd477778ba75e324bfec44d03a27a010dac7a2780']

Name

244c32c4809a5ea72dfd2a53d0c535f17ba3b33e4c3ee6ed229858d687a2563a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '244c32c4809a5ea72dfd2a53d0c535f17ba3b33e4c3ee6ed229858d687a2563a']

Name

241737842eb17676b3603e2f076336b7bc6304accef3057401264affb963bef8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '241737842eb17676b3603e2f076336b7bc6304accef3057401264affb963bef8']

Name

1e278cfe8098f3badedd5e497f36753d46d96d81edd1c5bee4fc7bc6380c26b3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1e278cfe8098f3badedd5e497f36753d46d96d81edd1c5bee4fc7bc6380c26b3']

Name

1d3d460b22f70cc26252673e12dfd85da988f69046d6b94602576270df590b2c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1d3d460b22f70cc26252673e12dfd85da988f69046d6b94602576270df590b2c']

Name

50.7.61.26

Description

- **Zip Code:** N/A - **ISP:** Fdcservers - **ASN:** 30058 - **Organization:** Fdcservers - **Is Crawler:** False - **Timezone:** Asia/Tokyo - **Mobile:** False - **Host:** 50.7.61.26 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** JP - **Region:** Tokyo - **City:** Tokyo - **Latitude:** 35.62 - **Longitude:** 139.74

Pattern Type

stix

Pattern

[ipv4-addr:value = '50.7.61.26']

Name

1c0853a5f86bb7eca48a36f07094188adb1a8893cd13309f91f669ba7c8ed124

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1c0853a5f86bb7eca48a36f07094188adb1a8893cd13309f91f669ba7c8ed124']

Name

18f4f14857e9b7e3aa1f6f21f21396abd5f421342b7f4d00402a4aff5a538fa1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '18f4f14857e9b7e3aa1f6f21f21396abd5f421342b7f4d00402a4aff5a538fa1']

Name

15412d1a6b7f79fad45bcd32cf82f9d651d9ccca082f98a0cca3ad5335284e45

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '15412d1a6b7f79fad45bcd32cf82f9d651d9ccca082f98a0cca3ad5335284e45']

Name

10b2a7c9329b232e4eef81bac6ba26323e3683ac1f8a99d3a9f8965da5036b6f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '10b2a7c9329b232e4eef81bac6ba26323e3683ac1f8a99d3a9f8965da5036b6f']

Name

0ff80e4db32d1d45a0c2afdfd7a1be961c0fbd9d43613a22a989f9024cc1b1e9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0ff80e4db32d1d45a0c2afdfd7a1be961c0fbd9d43613a22a989f9024cc1b1e9']

Name

0f0663fc26b18212485149e3e22c3dd4b8900ea8dca7c084dbe09fef02cfdade

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0f0663fc26b18212485149e3e22c3dd4b8900ea8dca7c084dbe09fef02cfdade']

Name

07e38ba00a0477367e63646bbd6e09053ab67939a9c70f062b12b42a2cde82fb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '07e38ba00a0477367e63646bbd6e09053ab67939a9c70f062b12b42a2cde82fb']

Name

05b63707ca3cad54085e521aee84c7472ff7b3fe05e22fd65c8e2ee6f36c6243

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '05b63707ca3cad54085e521aee84c7472ff7b3fe05e22fd65c8e2ee6f36c6243']

Name

01b09cb97a58ea0f9bf2b98b38b83f0cfc9f97f39f7bfd73a990c9b00bcdb66c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '01b09cb97a58ea0f9bf2b98b38b83f0cfc9f97f39f7bfd73a990c9b00bcdb66c']

Name

23.106.124.152

Description

- **Zip Code:** N/A - **ISP:** Leaseweb Asia - **ASN:** 59253 - **Organization:** Leaseweb Asia - **Is Crawler:** False - **Timezone:** Asia/Singapore - **Mobile:** False - **Host:** 23.106.124.152 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** SG - **Region:** Singapore - **City:** Singapore - **Latitude:** 1.34 - **Longitude:** 103.85

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.106.124.152']

Name

7e35078106bd59b739b1d1fb6ad16d56c3adaf9f10d2e206a1b9b23d64b25cd0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7e35078106bd59b739b1d1fb6ad16d56c3adaf9f10d2e206a1b9b23d64b25cd0']

Name

207.148.69.1

Description

- **Zip Code:** N/A - **ISP:** Vultr - **ASN:** 20473 - **Organization:** Vultr - **Is Crawler:** False - **Timezone:** Asia/Singapore - **Mobile:** False - **Host:** 207.148.69.1.vultrusercontent.com - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** SG - **Region:** Singapore - **City:** Singapore - **Latitude:** 1.31 - **Longitude:** 103.68

Pattern Type

stix

Pattern

[ipv4-addr:value = '207.148.69.1']

Name

50.7.61.27

Description

- **Zip Code:** N/A - **ISP:** Fdcservers - **ASN:** 30058 - **Organization:** Fdcservers - **Is Crawler:** False - **Timezone:** Asia/Tokyo - **Mobile:** False - **Host:** 50.7.61.27 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** JP - **Region:** Tokyo - **City:** Tokyo - **Latitude:** 35.62 - **Longitude:** 139.74

Pattern Type

stix

Pattern

[ipv4-addr:value = '50.7.61.27']

Name

207.148.75.122

Description

- **Zip Code:** N/A - **ISP:** Vultr - **ASN:** 20473 - **Organization:** Vultr - **Is Crawler:** False - **Timezone:** Asia/Singapore - **Mobile:** False - **Host:** 207.148.75.122.vultrusercontent.com - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** SG - **Region:** Singapore - **City:** Singapore - **Latitude:** 1.31 - **Longitude:** 103.68

Pattern Type

stix

Pattern

[ipv4-addr:value = '207.148.75.122']

Name

45.32.33.17

Description

Cobalt Strike botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.32.33.17']

Name

199.231.211.19

Pattern Type

stix

Pattern

[ipv4-addr:value = '199.231.211.19']

Name

118.99.6.202

Pattern Type

stix

Pattern

[ipv4-addr:value = '118.99.6.202']

Name

115.126.98.204

Pattern Type

stix

Pattern

[ipv4-addr:value = '115.126.98.204']

Name

d17fe5bc3042baf219e81cbbf991749dfcd8b6d73cf6506a8228e19910da3578

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd17fe5bc3042baf219e81cbbf991749dfcd8b6d73cf6506a8228e19910da3578']

Name

23.106.122.5

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.106.122.5']

Name

23.106.122.46

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.106.122.46']

Name

4cb020a66fdbc99b0bce2ae24d5684685e2b1e9219fbdfda56b3aace4e8d5f66

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4cb020a66fdbc99b0bce2ae24d5684685e2b1e9219fbdfda56b3aace4e8d5f66']

Vulnerability

Name
CVE-2021-22555
Name
CVE-2024-21412
Description
Microsoft Windows Internet Shortcut Files contains an unspecified vulnerability that allows for a security feature bypass.
Name
CVE-2022-21587
Description
Oracle E-Business Suite contains an unspecified vulnerability that allows an unauthenticated attacker with network access via HTTP to compromise Oracle Web Applications Desktop Integrator.
Name
CVE-2016-5195

Description
Race condition in mm/gup.c in the Linux kernel allows local users to escalate privileges.

Name
CVE-2023-32315

Description
Ignite Realtime Openfire contains a path traversal vulnerability that allows an unauthenticated attacker to access restricted pages in the Openfire Admin Console reserved for administrative users.

Name
CVE-2021-4034

Description
The Red Hat polkit pkexec utility contains an out-of-bounds read and write vulnerability that allows for privilege escalation with administrative rights.

Malware

Name
XDealer
Name
CORESHELL - S0137
Name
ShadowPad - S0596
Name
PlugX - S0013
Name
Cobalt Strike - S0154
Name
POISONPLUG.SHADOW
Description
[ShadowPad](https://attack.mitre.org/software/S0596) is a modular backdoor that was first identified in a supply chain compromise of the NetSarang software in mid-July 2017. The

malware was originally thought to be exclusively used by [APT41](https://attack.mitre.org/groups/G0096), but has since been observed to be used by various Chinese threat activity groups. (Citation: Recorded Future RedEcho Feb 2021)(Citation: Securelist ShadowPad Aug 2017)(Citation: Kaspersky ShadowPad Aug 2017)

Name

cobalt strike

Description

[Cobalt Strike](https://attack.mitre.org/software/S0154) is a commercial, full-featured, remote access tool that bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.(Citation: cobaltstrike manual) In addition to its own capabilities, [Cobalt Strike](https://attack.mitre.org/software/S0154) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: cobaltstrike manual)

Name

Kaba

Description

[PlugX](https://attack.mitre.org/software/S0013) is a remote access tool (RAT) with modular plugins that has been used by multiple threat groups.(Citation: Lastline PlugX Analysis)(Citation: FireEye Clandestine Fox Part 2)(Citation: New DragonOK)(Citation: Dell TG-3390)

Name

SOURFACE

Description

[CORESHELL](https://attack.mitre.org/software/S0137) is a downloader used by [APT28](https://attack.mitre.org/groups/G0007). The older versions of this malware are known as SOURFACE and newer versions as CORESHELL.(Citation: FireEye APT28) (Citation: FireEye APT28 January 2017)

Intrusion-Set

Name
Earth Krahang

Country

Name
American Samoa
Name
United States
Name
South Africa
Name
Central African Republic

Region

Name
Polynesia
Name
Oceania
Name
Northern America
Name
Americas
Name
Sub-Saharan Africa
Name
Africa

Sector

Name
Retail
Description
Distribution and sale of goods directly to the consumer.
Name
Manufacturing
Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.
Name
Technology
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.
Name

Healthcare

Description

Public and private entities involved in research, services and manufacturing activities related to public health.

Name

Government

Description

Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Name

Finance

Description

Public and private entities involved in the allocation of assets and liabilities over space and time.

Name

military

Description

Includes the military and all defense related-space activities.

Name

Defense

Description

Public and private entities involved in the conception and production of weapons and the planning and conducting of military operations.

Hostname

Value
www.security-microsoft.net
update.windows.server-microsoft.com
update.microsoft-setting.com
update.centos-yum.com
support.helpkaspersky.top
happy.gitweb.cloudns.nz
data-dev.helpkaspersky.top
cdn-dev.helpkaspersky.top

Domain-Name

Value
tfirstdaily.store
softupdate.xyz
gtldgtld.store

IPv4-Addr

Value
50.7.61.28
50.7.61.26
45.76.157.92
23.106.124.152
207.148.69.1
50.7.61.27
207.148.75.122
45.32.33.17
199.231.211.19
118.99.6.202
115.126.98.204
23.106.122.5
23.106.122.46

StixFile

Value
fff2f40e74ad7052ec9eeb08fb4aba2d807c3862beed80579944ed85456af1ab
ffef75582ad185c58135cf02e347c0ad6d46751fcfbb803dc3e70b73729e6136
fe4fad660bb44e108ab07d812f8b1bbf16852c1b881a5e721a9f811cae317f39
f6993e767306d4cbf676bf3c4a56fc2ad1d5cb6c4f67563f6de2f28b79f2b934
f66a6b49a23cf3cc842a84d955c0292e7d1c0718ec4e78d4513e18b6c53a94ac
f5b6c0d73c513c3c8efbcc967d7f6865559e90d59fb78b2b15394f22fd7315cb
f4ea99dc41cb7922d01955eef9303ec3a24b88c3318138855346de1e830ed09e
f34bd1d485de437fe18360d1e850c3fd64415e49d691e610711d8d232071a0b1
ef4a2cfe4d9d3495d4957a65299f608f7b823fab0699fded728fd3900c0b2bb4
ee41eb21f439b1168ae815ca067ee91d84d6947397d71e214edc6868dbf4f272
ebdf3d3e0867b29e66d8b7570be4e6619c64fae7e1fbd052be387f736c980c8e
ea140cc8da39014c1454c3f6a036d5f43aa26c215cb9981ab2b7076f2388b73e
e42466863837a655b814d2fb6aa2381369b8c5a9fe100e512085617f775dac36

e0f109836a025d4531ea895cebecc9bdefb84a0cc747861986c4bc231e1d4213

dd469fbf68f6bf71e495b3e497e31d17aa1d0af918a943f8637dd3304f840740

da1c9cb862b0be89819a94335eea8bf5ab56e08a1f4ca0ef92fe8d46fd2b1577

d462f3909c3e4b1a13b2fce4843a20f4622a256cd878d3345b3091e61f9ec1fc

d31d135bc450eafa698e6b7fb5d11b4926948163af09122ca1c568284d8b33b3

d310f5baa1c39ada9f60b85ed134b7cd99a04d9a8869f24ec9f3bd28ce9de519

d2cc1135c314f526f88fbe19f25d94899d52de7e3422f334437f32388d040d71

d176951b9ff3239b659ad57b729edb0845785e418852ecfeef1669f4c6fed61b

d096c3a67634599bc47151f0e01a7423a3eb873377371b2b928c0d4f57635a1f

ccd4a648cc2c4a5bbcd148f9c182f4c9595440a41dd3ea289a11609063c86a6d

c9d5dc956841e000bfd8762e2f0b48b66c79b79500e894b4efa7fb9ba17e4e9e

c377b79732e93f981998817e6f0e8664578b474445ba11b402c70b4b0357caab

c2bb47ac533d1413c829a1453b2b854b95aabebf1b26b446bd1ad0838f1e09de

c14f6ac5bcd8645eb80a612a6bf6d58c31b0e28e50be871f278c341ed1fa8c7c

bf830191215e0c8db207ea320d8e795990cf6b3e6698932e6e0c9c0588fc9eff

bc422a4e1b6a351ac6fe73d496015cfa6a9dbd5e38566c6f44a59faff83ee95a

bb6afc28d610bfddcd0cf3497c152c081f63137fea9914a1fd461a0706c74288

bb4e7b0c969895fc9836640b80e2bdc6572d214ba2ee55b77588f8a4eedea5a4

b8f2da1eefa09077d86a443ad688080b98672f171918c06e2b3652df783be03a

b4c470be7e434dac0b61919a6b0c5b10cf7a01a22c5403c4540afdb5f2c79fab

b3a6dfc196bdad381c18f9f861f8da3757479cec2a76b8e5908da5aaec072dd8

b19a46f99b649dc731ed5c8410bda7e0385d15e1b9aab1e467b05dccd7753865

b153e10c95bb8bfa6dbf5835067c5b45840f057a38ef9b8871b6dc40edcf601f

b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682

acfcf97ee4ff5cc7f5ecdc6f92ea132e29c48400ab6244de64f9b9de4368deb2

a99bf162a8588b2f318c9460aef78851bd64e4826c2cb124984d2ab357a6beea

a4f59d4d42e42b882068cacf8b70f314add963e2cbbf7a52e70df130bfe23dff

a36d64da109b47022591909362c3f9899efe5f0d8b902460e272761e2b75c75e

a2c3073fa5587f8a70d7def7fd8355e1f6d20eb906c3cd4df8c744826cb81d91

9d4e18ae979bdf6b57e685896b350b23c428d911eee14af133c3ee7d208f8a82

9ada058a558b7cadb238fc2c259f204369cd604e927f9712fd51262ca6987cb1

992d3df19c453a84b5b46c5742fb22686c65eb48cfc71b0bbc7e94c0ef13e66e

98b5b4f96d4e1a9a6e170a4b2740ce1a1dfc411ada238e42a5954e66559a5541

898a7527c065454ba9fad0e36469e12b214f5a3bd40a5ec7fcaf9b75afc34dce

82f7bcda95fcc0e690159a2fbd7b3e38ef3ff9105496498f86d1fa9ff4312846

8218c23361e9f1b25ee1a93796ef471ca8ca5ac672b7db69ad05f42eb90b0b8d

804387e43fdd1bd45b35e65d52d86882d64956b0a286e8721da402062f95a9e3

7e86d717a13d4c6ccce80098200331d5b963201ce0ffb59dadedbb555bf97d4c

7e5b05d29c3aa2aa178c3cc0338ba52b39dc89dafadeec7301f187db0b060372

7af402f4bd2b1a2d2d8b74fb7599860f3a90b7b6f66a519f2b4d31aeea2500aa

799214f6bf40056a1f0c903d5ac59e6216c49a5cd55e5c1a36a0f2c5637e345a

767694e220e5119425ed808bc0801a0070226148128 68e60962660863de42fa5

7102d6b76a4170203daa939072bba548960db436f85113cd1fca0bb554d95b3c

6fd7697efc137faf2d3ad5d63ffe4743db70f905a71dbed76207beeeb04732f2

6d03c6b7621990f84580eaa094393fbf896803c86779644506b115692b70bd64

6c006620062b40b22d00e7e73a93e6a7fa66ce720093b44b4a0f3ef809fa2716

6a4e32229e5ca41e8eca99cefe5beef3e3621c2199f8844b4d218c14b5481534

67ad30c3359b377d1964a5add97d2dc96b855940685131b302d5ba2c907ef355

63b7d8c4c740c54ab91db94dd89b2c8313ecb7ba13524c646fdb10facf5c470d

6302acdfce30cec5e9167ff7905800a6220c7dda495c0aae1f4594c7263a29b2

5e1839fed3562d559166f7f9d3e388cdd21da83b67ccb70fa4121825b91469d6

5b17bc2a89727700f94570b0dddc12b315db34dbbd79186177167abbb173cee5

5a6a0e01949799dc72c030b4ad8149446624dcd9645ba3eefda981c3fda26472

5a32bf21904387d469d4f8cdaff46048e99666fc9b4d74872af9379df7979bfe

57f64f170dfeaa1150493ed3f63ea6f1df3ca71ad1722e12ac0f77744fb1a829

521b3add2ab6cee5a5cfd53b78e08ef2214946393d2a156c674606528b05763a

50cdd2397836d33a8dc285ed421d9b7cc69e38ba0421638235206fd466299dab

4b653253049a65142f827706203de55f03abccbcddac3ed2171d79bf8186eda9

4aadf0aa60ffd932230c3e88437097a3ba85a2e5587c9b9d92c1ec172f795944

484578b6e7e427a151c309bdc00c90b1c0faf25a8581cace55e2c25ec34056e0

46b84d55c394c1c504c0fad8b5240bc0a183f5eda03e35d4f7f816bf48bff3e2

45e70dbed32cb723ea901c97d0c5682fe0e07e64485095c3e5bbccc86059384e

4529f3751102e7c0a6ec05c6a987d0cc5edc08f75f287dd6ac189abbd1282014

44b0479dd2debc68480c4cd4759466bf1aac8d3405b99071a61854cb63500448

42fecaaf47ed5606d4e4885ce821702a83bbaa4602a13ab0e9b933a04e373956

3f0aa01ed70bc2ab29557521a65476ec2ff2c867315067cc8a5937d63bcbe815

3a3db15bd60f30293cfdf1ca7e159b8040d380665cc0857aed098b471be77030

36acdaceb9abfcf9923378c44037cc5df8aac03406d082d552e96462121c4ac1

363f5d92a2692898ed7d5d2caa5e8f51f4db466d0b9134328aafad359e027544

35f16e469047cf4ef78f87a616d26ec09e3d6a3d7a51415ea34805549a41dcfa

2f3d89e8db70e7560868c4cf7f03aafa4cd703a13d1d6f814028469806cb6bd7

2e9da6d50f8b73a00310f91cf1fc79e4804265a08028dcb6272623440bb47497

2e850cb2a1d06d2665601cefd88802ff99905de8bc4ea348ea051d4886e780ee

2e3645c8441f2be4182869db5ae320da00c513e0cb643142c70a833f529f28aa

2e012ba20ecb553745f7719bd477778ba75e324bfec44d03a27a010dac7a2780

244c32c4809a5ea72dfd2a53d0c535f17ba3b33e4c3ee6ed229858d687a2563a

241737842eb17676b3603e2f076336b7bc6304accef3057401264affb963bef8

1e278cfe8098f3badedd5e497f36753d46d96d81edd1c5bee4fc7bc6380c26b3

1c0853a5f86bb7eca48a36f07094188adb1a8893cd13309f91f669ba7c8ed124

1d3d460b22f70cc26252673e12dfd85da988f69046d6b94602576270df590b2c

18f4f14857e9b7e3aa1f6f21f21396abd5f421342b7f4d00402a4aff5a538fa1

15412d1a6b7f79fad45bcd32cf82f9d651d9ccca082f98a0cca3ad5335284e45

10b2a7c9329b232e4eef81bac6ba26323e3683ac1f8a99d3a9f8965da5036b6f

0ff80e4db32d1d45a0c2afdfd7a1be961c0fbd9d43613a22a989f9024cc1b1e9

07e38ba00a0477367e63646bbd6e09053ab67939a9c70f062b12b42a2cde82fb

0f0663fc26b18212485149e3e22c3dd4b8900ea8dca7c084dbe09fef02cfdade

05b63707ca3cad54085e521aee84c7472ff7b3fe05e22fd65c8e2ee6f36c6243

01b09cb97a58ea0f9bf2b98b38b83f0cfc9f97f39f7bfd73a990c9b00bcdb66c

7e35078106bd59b739b1d1fb6ad16d56c3adaf9f10d2e206a1b9b23d64b25cd0

d17fe5bc3042baf219e81cbbf991749dfcd8b6d73cf6506a8228e19910da3578

4cb020a66fdbc99b0bce2ae24d5684685e2b1e9219fbdfda56b3aace4e8d5f66

External References

- https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/c/earth-krahang-exploits-intergovernmental-trust-to-launch-cross-government-attacks/ioc_earth_krahang.txt
- https://www.trendmicro.com/en_us/research/24/c/earth-krahang.html
- https://otx.alienvault.com/pulse/65f818642d29b84d812a6654