Oct 05 2023

NETMANAGEIT

Intelligence Report

LightSpy mAPT Mobile Payment System Attack

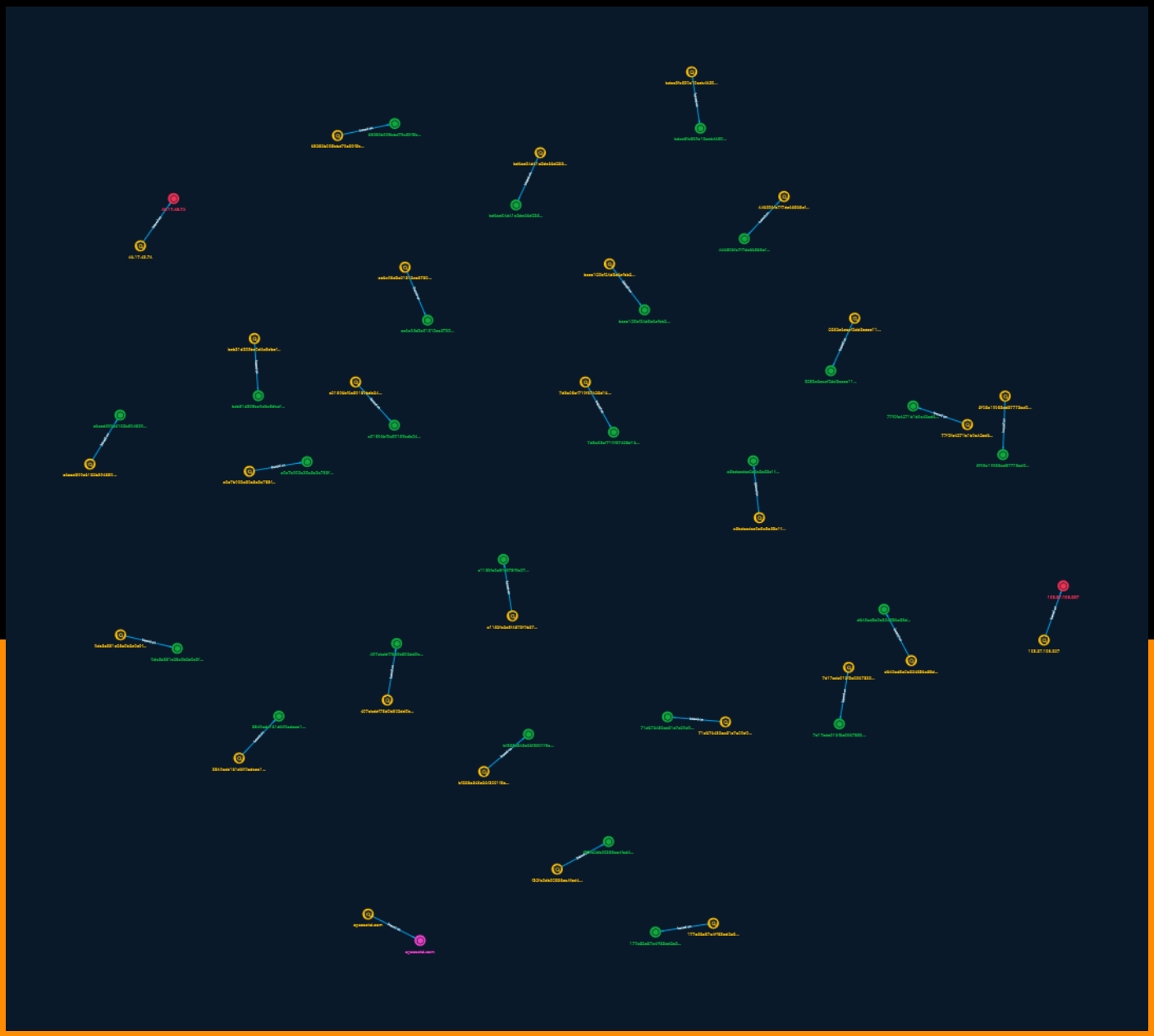

Table of contents

Overview

Entities

Observables

External References

Overview

Description

ThreatFabric tied DragonEgg Android spyware to sophisticated iOS targeted malware LightSpy and revealed previously unknown unique additional payloads.

Confidence

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

15 / 100

Content

N/A

Indicator

Name

46.17.43.74

Description

ISP: LLC Baxet **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEmETbuGsIcadwtj6pXpK0RN LnkBnCdGihEU6rS9rqeFo7h3SKoRmjP7vB4jRDNUZtZMIxZfiAFS2GjVa+y4P1c= Fingerprint: 7a:d6:68:1a:73:22:38:0c:6b:74:00:9a:79:0b:9d:d1 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '46.17.43.74']

Name

5f93a19988cd87775ad0822a35da98d1abcc36142fd63f140d488b30045bdc00

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5f93a19988cd87775ad0822a35da98d1abcc36142fd63f140d488b30045bdc00']

Name

407abddf78d0b802dd0b8e733aee3eb2a51f7ae116ae9428d554313f12108a4c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '407abddf78d0b802dd0b8e733aee3eb2a51f7ae116ae9428d554313f12108a4c']

Name

bace120bf24d8c6cfbb2c8bfeed1365112297740e2a71a02ea2877f5ffc6b325

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bace120bf24d8c6cfbb2c8bfeed1365112297740e2a71a02ea2877f5ffc6b325']

Name

71d676480ec51c7e09d9c0f2accb1bdce34e16e929625c2c8a0483b9629a1486

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '71d676480ec51c7e09d9c0f2accb1bdce34e16e929625c2c8a0483b9629a1486']

Name

c0c7b902a30e5a3a788f3ba85217250735aaaf125a152a32ee603469e2dfb39e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c0c7b902a30e5a3a788f3ba85217250735aaaf125a152a32ee603469e2dfb39e']

Name

bd6ec04d41a5da66d23533e586c939eece483e9b105bd378053e6073df50ba99

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bd6ec04d41a5da66d23533e586c939eece483e9b105bd378053e6073df50ba99']

Name

e1152fe2c3f4573f9b27ca6da4c72ee84029b437747ef3091faa5a4a4b9296be

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e1152fe2c3f4573f9b27ca6da4c72ee84029b437747ef3091faa5a4a4b9296be']

Name

68252b005bbd70e30f3bb4ca816ed09b87778b5ba1207de0abe41c24ce644541

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '68252b005bbd70e30f3bb4ca816ed09b87778b5ba1207de0abe41c24ce644541']

Name

77f0fc4271b1b9a42cd6949d3a6060d912b6b53266e9af96581a2e78d7beb87b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '77f0fc4271b1b9a42cd6949d3a6060d912b6b53266e9af96581a2e78d7beb87b']

Name

spaceskd.com

Pattern Type

stix

Pattern

[domain-name:value = 'spaceskd.com']

Name

7d8a08af719f87425d1643d59979d4a3ef86a5fc81d1f06cfa2fd8c18aeb766b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7d8a08af719f87425d1643d59979d4a3ef86a5fc81d1f06cfa2fd8c18aeb766b']

Name

d640ad3e0a224536e58d771fe907a37be1a90ad26bf0dc77d7df86d7a6f7ca0e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd640ad3e0a224536e58d771fe907a37be1a90ad26bf0dc77d7df86d7a6f7ca0e']

Name

c6ccd599c6122b894839e12d080062de0fa59c4cd854b255e088d22e11433ef6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c6ccd599c6122b894839e12d080062de0fa59c4cd854b255e088d22e11433ef6']

Name

2282c6caef2dd5accc1166615684ef2345cf7615fe27bea97944445ac48d5ce4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2282c6caef2dd5accc1166615684ef2345cf7615fe27bea97944445ac48d5ce4']

Name

f32fa0db00388ce4fed4e829b17e0b06ae63dc0d0fac3f457b0f4915608ac3b5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f32fa0db00388ce4fed4e829b17e0b06ae63dc0d0fac3f457b0f4915608ac3b5']

Name

bcb31d308ba9d6a8dbaf8b538cee4085d3ef37c5cb19bf7e7bed3728cb132ec1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bcb31d308ba9d6a8dbaf8b538cee4085d3ef37c5cb19bf7e7bed3728cb132ec1']

Name

103.27.108.207

Description

ISP: TOPWAY GLOBAL LIMITED **OS:** Ubuntu ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDRqJ47stVb8UFoYfb3nkI/59wkhkr8jKFFEObNiCdyCW1oTe1Zhv91MXnxDnroerqv5tUoPYL9IJ+aeBYZzLCKMmgkBuEDxUDbKbQUOpJ7PwNUC1/l8b0hKDjmpP5h1aHWkGjq5HbHcckeQ2e0usMqrm8PxEYTXcMYK8vefkTp8l39zAP/u5TvsLBm4f87wNmjuYteMEHmOqX7uH4OeNADdt7vux+9ptXFgrG/r493SYbTnjKfMEMU5EJWpUotWGMuxd3tiyHuIqDj7QwKl2pK9lMTfBU+r1BR6GJUaSEbTDaNwcvhtvV6UaE743Dedu0o0No49FHwolUYMRYfJkzB Fingerprint: 4e:a8:89:ac:fc:ac:9d:5c:e8:cb:23:7a:4f:24:5f:79 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **443:** ``` ``` ---------- **6000:** ``` ``` ---------- **9002:** ``` HTTP/1.1 404 Not Found Server: TornadoServer/6.1 Content-Type: text/html; charset=UTF-8 Date: Thu, 28 Sep 2023 13:07:15 GMT Content-Length: 69 404: Not Found ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.27.108.207']

Name

3849adc161d699edaca161d5b6335dfb7e5005056679907618d5e74b9f78792f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3849adc161d699edaca161d5b6335dfb7e5005056679907618d5e74b9f78792f']

Name

bdcc5fc529e12ecb465088b0a975bd3a97c29791b4e55ee3023fa4f6db1669dc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bdcc5fc529e12ecb465088b0a975bd3a97c29791b4e55ee3023fa4f6db1669dc']

Name

177e52c37a4ff83cd2e5a24ff87870b3e82911436a33290135f49356b8ee0eb1

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '177e52c37a4ff83cd2e5a24ff87870b3e82911436a33290135f49356b8ee0eb1']

Name

a01896bf0c39189bdb24f64a50a9c608039a50b068a41ebf2d49868cc709cdd3

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'a01896bf0c39189bdb24f64a50a9c608039a50b068a41ebf2d49868cc709cdd3']
Name
7d17cdc012f3c2067330fb200811a7a300359c2ad89cdcf1092491fbf5a5a112
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '7d17cdc012f3c2067330fb200811a7a300359c2ad89cdcf1092491fbf5a5a112']
Name
bf338e548c26f3001f8ad2739e2978586f757777f902e5c4ab471467fd6d1c04
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'bf338e548c26f3001f8ad2739e2978586f757777f902e5c4ab471467fd6d1c04']

Name

cc6a95d3e01312ca57304dc8cd966d461ef3195aab30c325bee8e5b39b78ae89

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cc6a95d3e01312ca57304dc8cd966d461ef3195aab30c325bee8e5b39b78ae89']

Name

e5bdeedac2c5a3e53c1fdc07d652c5d7c9b346bcf86fc7184c88603ff2180546

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e5bdeedac2c5a3e53c1fdc07d652c5d7c9b346bcf86fc7184c88603ff2180546']

Name

9da5c381c28e0b2c0c0ff9a6ffcd9208f060537c3b6c1a086abe2903e85f6fdd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9da5c381c28e0b2c0c0ff9a6ffcd9208f060537c3b6c1a086abe2903e85f6fdd']

Name

446506fa7f7dc66568af4ab03e273ff25ee1dc59d0440086c1075d030fe72b11

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '446506fa7f7dc66568af4ab03e273ff25ee1dc59d0440086c1075d030fe72b11']

Domain-Name

Value
spaceskd.com

StixFile

Value
a01896bf0c39189bdb24f64a50a9c608039a50b068a41ebf2d49868cc709cdd3
3849adc161d699edaca161d5b6335dfb7e5005056679907618d5e74b9f78792f
bdcc5fc529e12ecb465088b0a975bd3a97c29791b4e55ee3023fa4f6db1669dc
f32fa0db00388ce4fed4e829b17e0b06ae63dc0d0fac3f457b0f4915608ac3b5
446506fa7f7dc66568af4ab03e273ff25ee1dc59d0440086c1075d030fe72b11
bf338e548c26f3001f8ad2739e2978586f757777f902e5c4ab471467fd6d1c04
71d676480ec51c7e09d9c0f2accb1bdce34e16e929625c2c8a0483b9629a1486
407abddf78d0b802dd0b8e733aee3eb2a51f7ae116ae9428d554313f12108a4c
bace120bf24d8c6cfbb2c8bfeed1365112297740e2a71a02ea2877f5ffc6b325
9da5c381c28e0b2c0c0ff9a6ffcd9208f060537c3b6c1a086abe2903e85f6fdd
68252b005bbd70e30f3bb4ca816ed09b87778b5ba1207de0abe41c24ce644541
7d8a08af719f87425d1643d59979d4a3ef86a5fc81d1f06cfa2fd8c18aeb766b
c6ccd599c6122b894839e12d080062de0fa59c4cd854b255e088d22e11433ef6

77f0fc4271b1b9a42cd6949d3a6060d912b6b53266e9af96581a2e78d7beb87b

cc6a95d3e01312ca57304dc8cd966d461ef3195aab30c325bee8e5b39b78ae89

c0c7b902a30e5a3a788f3ba85217250735aaaf125a152a32ee603469e2dfb39e

2282c6caef2dd5accc1166615684ef2345cf7615fe27bea97944445ac48d5ce4

bd6ec04d41a5da66d23533e586c939eece483e9b105bd378053e6073df50ba99

d640ad3e0a224536e58d771fe907a37be1a90ad26bf0dc77d7df86d7a6f7ca0e

177e52c37a4ff83cd2e5a24ff87870b3e82911436a33290135f49356b8ee0eb1

e1152fe2c3f4573f9b27ca6da4c72ee84029b437747ef3091faa5a4a4b9296be

5f93a19988cd87775ad0822a35da98d1abcc36142fd63f140d488b30045bdc00

bcb31d308ba9d6a8dbaf8b538cee4085d3ef37c5cb19bf7e7bed3728cb132ec1

e5bdeedac2c5a3e53c1fdc07d652c5d7c9b346bcf86fc7184c88603ff2180546

7d17cdc012f3c2067330fb200811a7a300359c2ad89cdcf1092491fbf5a5a112

IPv4-Addr

Value
46.17.43.74
103.27.108.207

External References

- https://otx.alienvault.com/pulse/651e894c542f6ffb37006070
- https://www.threatfabric.com/blogs/lightspy-mapt-mobile-payment-system-attack#attribution