NETMANAGEIT

Intelligence Report

BadBazaar espionage tool targets Android users via trojanized Signal and Telegram apps

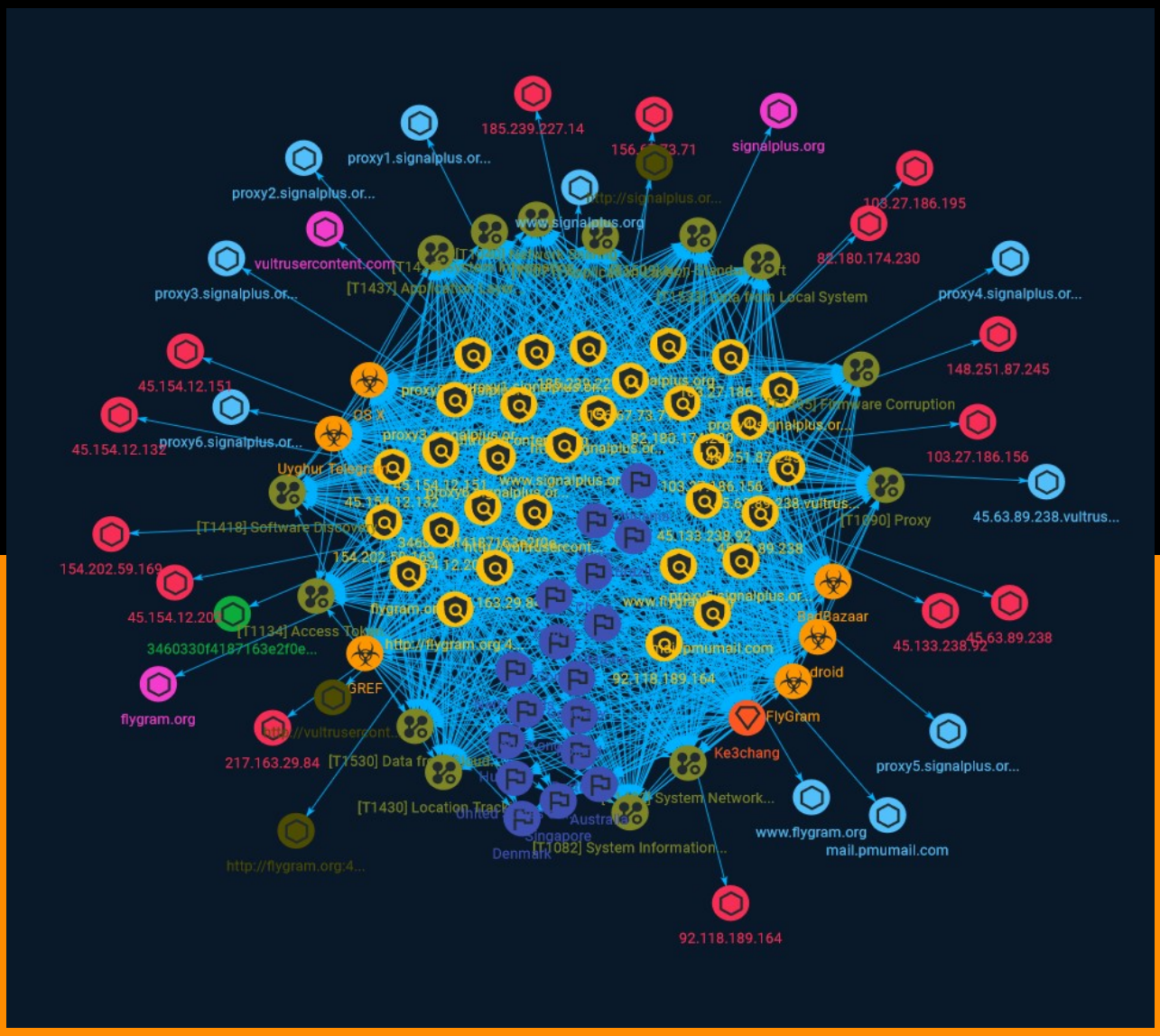

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Research has identified two campaigns targeting Android users via trojanized Signal and Telegram apps and a malware family that has previously been used to target Uyghurs and other Turkic ethnic minorities.

Confidence

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

15 / 100

Indicator

Name

45.133.238.92

Description

ISP: XNNET LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **3389:** ``` HTTP/1.1 407 Proxy Authentication Required Server: Proxy Proxy-Authenticate: Basic realm="CCProxy Authorization" Connection: Close Proxy-Connection: Close Content-Length: 263 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.133.238.92']

Name

3460330f4187163e2f0ee96c034a2db3c386de3dff5a8b6c8180ab3260bc705b

Description

xor_0x20_xord_javascript SHA256 of e368db837edf340e47e85652d6159d6e90725b0d

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '3460330f4187163e2f0ee96c034a2db3c386de3dff5a8b6c8180ab3260bc705b']
Name
vultrusercontent.com
Pattern Type
stix
Pattern
[domain-name:value = 'vultrusercontent.com']
Name
http://vultrusercontent.com
Pattern Type
stix
Pattern
[url:value = 'http://vultrusercontent.com']
Name

http://signalplus.org:4332

Pattern Type

stix

Pattern

[url:value = 'http://signalplus.org:4332']

Name

103.27.186.156

Description

ISP: Starry Network Limited **OS:** None ---------- Hostnames: - proxy6.signalplus.org ---------- Domains: - signalplus.org ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.0 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQC6nMzEmUZ79T5mUKkWVi/kCy/a9GvOW4Wp5eMg7bG2xcu3 hFEyh2L4+YZaM1Tiy0e/YKxrobP/ItB2DkJrwOBH4lCUECPx80tmj4gRRyi5UGVWmp9Djidrlevj 5dZMJV7B/ZBuyJerg5FZq/Y/TH28RLAy9BllXJpx0J8foyLNOt4FEYnNNa6ojpUTdf2EuNHUdt10 nqk3oedohDhEC4XIRavQUfvFn1fOYktoLRdENiWjzwqTvAeiFs+GrlKQ/zBVYttR5N4Be1b49QaH WmPXVez3oGafA8UA22WlQ0eL3Q6LrdGdXJUpo++HA56PDFqBm8TbPGWF/d1wV8Q2rKCx9awEmQME aSvrs9fT16hfKQ3ATSiSLjMxnzRQSZSYEd/08tjPSDXu+2mVisvClM7xTk5Y+qRs9lN144WzP8pK 0wKj2hG1Uz7MmpBhAJUquYifQn4koHSvLU8N7CmKLEif2equ4Z2f50JBq1FGKHLBJZje/FLitMunXlo5R7AFuG8= Fingerprint: 7f:28:93:78:8a:03:5d:75:a3:0f:c0:0c:bb:d1:43:46 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: aes256-gcm@openssh.com chacha20-poly1305@openssh.com aes256-ctr aes256-cbc aes128-gcm@openssh.com aes128-ctr aes128-cbc MAC Algorithms: hmac-sha2-256-etm@openssh.com hmac-sha1-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha2-256 hmac-sha1 umac-128@openssh.com hmac-sha2-512 Compression Algorithms: none zlib@openssh.com ``` ---------- **443:** ```

``` HEARTBLEED: 2023/08/31 07:11:57 103.27.186.156:443 - ERROR: write tcp 103.27.186.156:443: broken pipe ----------

**Pattern Type**

stix

**Pattern**

[ipv4-addr:value = '103.27.186.156']

**Name**

92.118.189.164

**Description**

**ISP:** CNSERVERS LLC **OS:** None ---------- Hostnames: - proxy2.signalplus.org - 92.118.189.164.static.xtom.com ---------- Domains: - signalplus.org - xtom.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.0 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDSqJ3xjLjcxAemd3FbvLbr0GGdLKCb3C5PujJYgx0dKxRwv4/zHt44NRlAvG0q+ADfxtSqO4lEbw4hDo7ycUf9CnnxEVYhpAs1hG+P61QdICMO67O8i/0ZGBvcBrfSuTl7r49mtCPmQWouiCS2pziHBOZCoT8q3LovPKOHFcbgrIFjNU9DRkV2fw6SIykbV5x4HtGk1OgRC1rL9PZvqdO+1Am9WiZjz0uSxsuBC5LYsaEy/K5AWh1rfc94YldljAPOI/i+HyVpaxuFBTtWaJFGmxfsUgVC2D3+9OK9Wl0sOBadnlhcqsTBmwMR2QJAIe902dgsPgUIWpkRJMKMmSPcivKRQ7PW CVtca6ZoWyxtBU6kpy6mt0YlNlP4/ EAUPeBIUo8XsPU81OPpAtBH6NU75l7rVHSzBbTxyVArkKnC yq1dvFwBaEDqRl/3jAQs/R9XOacdzmmNWy5f6GopAyWI6wqdC/mZ2GEwl5rkva7KuS7EQPDikAM6 X2tPU+XcSTU= Fingerprint: 00:cc:7a:e4:b9:e2:9b:57:28:ac:a6:5f:f8:9c:b5:78 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: aes256-gcm@openssh.com chacha20-poly1305@openssh.com aes256-ctr aes256-cbc aes128-gcm@openssh.com aes128-ctr aes128-cbc MAC Algorithms: hmac-sha2-256-etm@openssh.com hmac-sha1-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha2-256 hmac-sha1 umac-128@openssh.com hmac-sha2-512 Compression
```

Algorithms: none zlib@openssh.com ``` ---------- **443:** ``` ``` HEARTBLEED: 2023/08/28 11:50:01 92.118.189.164:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '92.118.189.164']

Name

proxy2.signalplus.org

Pattern Type

stix

Pattern

[hostname:value = 'proxy2.signalplus.org']

Name

45.63.89.238

Description

ISP: The Constant Company, LLC **OS:** None ---------- Hostnames: - 45.63.89.238.vultrusercontent.com - beginner.sp1der.top ---------- Domains: - vultrusercontent.com - sp1der.top ---------- Services: **21:** ``` 220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220-You are user number 1 of 50 allowed. 220-Local time is now 06:06. Server port: 21. 220-This is a private system - No anonymous login 220-IPv6 connections are also welcome on this server. 220 You will be disconnected after 15 minutes of inactivity. 421 Unable to read the indexed puredb file (or old format detected) - Try pure-pw mkdb 211-Extensions supported: UTF8 EPRT IDLE MDTM SIZE MFMT

REST STREAM MLST type*;size*;sizd*;modify*;UNIX.mode*;UNIX.uid*;UNIX.gid*;unique*; MLSD PRET AUTH TLS PBSZ PROT TVFS ESTA PASV EPSV SPSV ESTP 211 End. ``` ---------- **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQC4BjTs8Hj5gvFGPFZw5+5/VZruw9dPtusCA0sZIgnC4mI6 vvuQCIdy+ieD7a2Bb+8bATnnQT+OkbSIVgqfmN+2gCV6KiporcsXNi2WJcZT6UUV2BHI9uYxqhKO YXP+WL6Xagj6zmteSFM1dibURsrqzCLV9oVKrOG2Td/YgdnqjuMd12XFhJmlhWhuFhqXlesvjeMJ 9RkAzHzefTX/ZWLl76WP4qTWTDif6YiQiu68YZzRyhy/RmYBHbVDcx44AlFZJ1rA+cJala4Po2uk 1QxsLR408XQdEOV4rDGSZcwNWGC+YDVdaJqQ9iKtUrpsHumODtNpj2lXcv9IQXHkUoQEBN0riYs h 1FW+axUtDaoTYoJlfGzxQ5khpOwkpJA7Q1NU1o3p7mYzOLzqRJHMReUZhNbYWUQ5pISxnx6A6n/ R cRMI0v8hFodPvNxbrrVmnuSKJ4/ S5turnwwfW8iFGYRv3me057ONRWh7DW45Axw6UVLyMsht3AvZ E2Y8airxa80= Fingerprint: df:c9:76:42:37:d3:78:ba:96:45:f9:9a:b5:c5:ac:d0 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 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa 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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Mon, 28 Aug 2023 11:08:36 GMT Content-Type: text/html Content-Length: 138 Last-Modified: Fri, 23 Jun 2023 11:05:29 GMT Connection: keep-alive ETag: "64957c79-8a" Accept-Ranges: bytes ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx Date: Fri, 25 Aug 2023 20:12:14 GMT Content-Type: text/html Content-Length: 4268 Last-Modified: Tue, 11 Jul 2023 05:07:45 GMT Connection: keep-alive Vary: Accept-Encoding ETag: "64ace3a1-10ac" Strict-Transport-Security: max-age=31536000 Accept-Ranges: bytes ``` HEARTBLEED: 2023/08/25 20:12:30 45.63.89.238:443 - SAFE ---------- **3306:** ``` MySQL: Error Message: Host '224.81.231.35' is not allowed to connect to this MySQL server Error Code: 1130 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.63.89.238']

Name

proxy6.signalplus.org

Pattern Type

stix

Pattern

[hostname:value = 'proxy6.signalplus.org']

Name

signalplus.org

Pattern Type

stix

Pattern

[domain-name:value = 'signalplus.org']

Name

www.flygram.org

Pattern Type

stix

Pattern

[hostname:value = 'www.flygram.org']

Name

www.signalplus.org

Pattern Type

stix

Pattern

[hostname:value = 'www.signalplus.org']

Name

82.180.174.230

Description

ISP: Hostinger International Limited **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 403 Forbidden Connection: Keep-Alive Keep-Alive: timeout=5, max=100 cache-control: private, no-cache, no-store, must-revalidate, max-age=0 pragma: no-cache content-type: text/html content-length: 699 date: Wed, 30 Aug 2023 22:25:14 GMT server: LiteSpeed platform: hostinger ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '82.180.174.230']

Name

45.154.12.202

Description

ISP: MOACK.Co.LTD **OS:** None ---------- Hostnames: - proxy4.signalplus.org ---------- Domains: - signalplus.org ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.0 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCYt8Tm++sHlVJOiTJTdGaXmmU/C64HjDyVt6UORX0Z1zOP vVRboyllIWkQ2gVek0QR/u4B7ZZTW9DbrSK/zj25loXMRzycDgPGFhXVcKiHpQkspcUJk5sZ/88+ FG0xX2js//ivJwmcc5tV08pX02Q2KkbTXFawW+ThBNzn9nmzepilUcfuL5nRNbir62CgRGicV3HZJl8Tz0wF9929rQ0E1l3XHHdAFjlnicm1JpQ28FIXBwF59mhOBiNNuyTN2rjxEv8+RQZk2DUZp0miGH1gDVXqO/eKRaGC4YTcQcTmNB05EibtOS+GRlySMJ9/Ys3w7wRSskzN7yJkcYGBAQJSnKJVwcLJuvy5+kqEkU6OevjtmeqieDiPBljyDil+yB8yLqsbKqPScAznb/NvZpZBfREeIUYGTIXh1s8uz/rmxzs3NcQUq1HqEDyusQicGbMythltUUGkV7hnNhB7lKrKKeQRejfGsw0iqTz24vRmR0GPQkVfHoLwQxQarvSxen8= Fingerprint: 90:fc:62:40:39:ac:5d:fd:53:c1:45:5f:b0:74:ad:65 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: aes256-gcm@openssh.com chacha20-poly1305@openssh.com aes256-ctr aes256-cbc aes128-gcm@openssh.com aes128-ctr aes128-cbc MAC Algorithms: hmac-sha2-256-etm@openssh.com hmac-sha1-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha2-256 hmac-sha1 umac-128@openssh.com hmac-sha2-512 Compression Algorithms: none zlib@openssh.com ``` ---------- **443:** ``` ``` HEARTBLEED: 2023/08/14 23:41:58 45.154.12.202:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.154.12.202']

Name

156.67.73.71

Description

ISP: Hostinger International Limited **OS:** None ---------- Hostnames: - hstgr.io ---------- Domains: - hstgr.io ---------- Services: **80:** ``` HTTP/1.1 403 Forbidden Connection: Keep-Alive Keep-Alive: timeout=5, max=100 cache-control: private, no-cache, no-store, must-revalidate, max-age=0 pragma: no-cache content-type: text/html content-length: 699 date: Thu, 03 Aug 2023 05:50:30 GMT server: LiteSpeed platform: hostinger ``` ---------- **443:** ``` HTTP/1.1 403 Forbidden Connection: Keep-Alive Keep-Alive: timeout=5, max=100 cache-control: private, no-cache, no-store, must-revalidate, max-age=0 pragma: no-cache content-type: text/html content-length: 699 date: Mon, 28 Aug 2023 14:36:37 GMT server: LiteSpeed platform: hostinger alt-svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000, h3-Q050=":443"; ma=2592000, h3-Q046=":443"; ma=2592000, h3-Q043=":443"; ma=2592000, quic=":443"; ma=2592000; v="43,46" ``` HEARTBLEED: 2023/08/28 14:37:03 156.67.73.71:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '156.67.73.71']

Name

45.63.89.238.vultrusercontent.com

Pattern Type

stix

Pattern

[hostname:value = '45.63.89.238.vultrusercontent.com']

Name

45.154.12.132

Description

CC=GB ASN=AS138195 MOACK.Co.LTD

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.154.12.132']

Name

103.27.186.195

Description

ISP: Starry Network Limited **OS:** None ---------- Hostnames: - proxy5.signalplus.org ---------- Domains: - signalplus.org ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.0 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQD5baagHZzIsxfF0FYWjfsCu0ptoktZyT4vKobExHCrvFi4 fPJCk0MczeeKK6YQeEcSmYCJ9UneGwfpul84/Rbm1ohc+FHRCPlMHtGDF9XkLcrdYGbxDUgt3Z4k xqHD75oAN+Ztz+Py0g7a5ewGlhm1o5s8ngPe33sDupAhL107ZHQnnsNz7ef0qZCCOrECRnlOIpXT NwYxTn16sh1kaM5XcvLp5snkossA8v96u+FAj2ATMfG72cHxe9OQVrRsfHYv5hUob2p3o+Z0a4b0 rI2seJKU3NbEg6gYxmdUkwc2KiCN9L+4jGMpYH4I5OXKpvIn428KQbozf6R0HH5uQuc1HcT1grTg XuXvnQCxn4ySUn/HU6wXQWvqmqw7EZP9wt8Icybo5J976vCEe5gnLz9KUmK5UAEM/ EtgFabil6EM YAdMFgPk3wn2dZSBVf4IOBYWc1CfbXzwWqLt7zayHu6lSpePG6xOD0+eSrV+TrpAVTSWW+6AMB hx T51LBsa5BAs= Fingerprint: 95:3e:6f:4f:7c:cf:ec:dc:df:21:42:59:21:dd:24:95 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: aes256-gcm@openssh.com chacha20-poly1305@openssh.com aes256-ctr aes256-cbc aes128-gcm@openssh.com aes128-ctr aes128-cbc MAC Algorithms: hmac-sha2-256-etm@openssh.com hmac-sha1-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha2-256 hmac-sha1 umac-128@openssh.com hmac-

sha2-512 Compression Algorithms: none zlib@openssh.com ``` ---------- **443:** ``` ``` HEARTBLEED: 2023/08/19 04:37:35 103.27.186.195:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.27.186.195']

Name

217.163.29.84

Description

CC=DE ASN=AS20473 AS-CHOOPA

Pattern Type

stix

Pattern

[ipv4-addr:value = '217.163.29.84']

Name

proxy3.signalplus.org

Pattern Type

stix

Pattern

[hostname:value = 'proxy3.signalplus.org']

Name

148.251.87.245

Description

ISP: Hetzner Online GmbH **OS:** None ---------- Hostnames: - static.245.87.251.148.clients.your-server.de ---------- Domains: - your-server.de ---------- Services: **3389:** ``` ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '148.251.87.245']

Name

154.202.59.169

Description

ISP: CNSERVERS LLC **OS:** None ---------- Hostnames: - proxy1.signalplus.org ---------- Domains: - signalplus.org ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.0 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDcx4ckz6hI7VKWTImis49Jpp+KqrzhYOcDxRF9VdLPG+HGxgqet7+Jj3faDHKNcw4yMbCsP+uZkVnvXTqS18FCmgzIdzeZRPsJvBXruZtZWqxbSi66lqVUpem5BWbU4G6ZBDRPj7NIgmPoPOIOz7gq373w9EvM/5OgQ/7YIJRo22oB9irsk7h0IACLZ8vjdAJbDRYV+2Gak6W5ppKLxWJd7ex1HMKKq6uqvBKJP01HFsYnwg2ptHC+zwtUb5PLnsD5jr0MevJCsJbf6H1J18VvYf5/s+Y2Cd6X5UmdPBgqaH9m/hRRHziOWN5UM3jAkQCozt0n8sao7TLfQnNh1lwy69H8OYrI 5O7+lL+yxJ0oPH389A/

KAl+BLHC5kX0mbdqGOe+EOWlM3ZIS+i6ePKgD34fgHrcchwJ/OAKxPUNt hZ1uAQ4dpj8mgymFgVKOJ7XbPyXnQabTrauxe0ad9EYw6/0NrMj/CaUYW1v6/uh1tDGWw0d0/ tlE 5GtN46uzZjs= Fingerprint: 80:f2:91:77:8d:0c:db:67:40:2d:5f:48:50:d1:d9:0a Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: aes256-gcm@openssh.com chacha20-poly1305@openssh.com aes256-ctr aes256-cbc aes128-gcm@openssh.com aes128-ctr aes128-cbc MAC Algorithms: hmac-sha2-256-etm@openssh.com hmac-sha1-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha2-256 hmac-sha1 umac-128@openssh.com hmac-sha2-512 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 404 Not Found Server: nginx/1.18.0 Date: Thu, 31 Aug 2023 06:44:03 GMT Content-Type: text/html Content-Length: 555 Connection: keep-alive ``` ---------- **443:** ``` ``` HEARTBLEED: 2023/08/30 03:30:11 154.202.59.169:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '154.202.59.169']

Name

185.239.227.14

Description

CC=HK ASN=AS134835 Starry Network Limited

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.239.227.14']

Name

mail.pmumail.com

Pattern Type

stix

Pattern

[hostname:value = 'mail.pmumail.com']

Name

45.154.12.151

Description

ISP: MOACK.Co.LTD **OS:** None ---------- Hostnames: - proxy3.signalplus.org ---------- Domains: - signalplus.org ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.0 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDUyoBnkkDz90ppkgdUZBrBEK7GMa1+nqrnV1rMWsnZa RFf q46NipTT96k3SsHwlQPGkdwUO7z/gHVPFW7eO1RbrrRuqjfBh/ Df7BgjpRGdWt8e0li1OpZKVGBd HFcjpZ6Szn38CNa8kPrYbEIeIThhrqjBaaLkkgi8s786eachP1UzAVUQGWDCUjlGmCkW/RjP129i aTvqFUZfRxd1Ql56RWXgpXyVvzWZy0AOPwkekeONwABq/ 7wPCipJGYhNXSA9riDTSpnom2fbsLvW 2UlZjnXn0GD1rkDYDWcVkwh/ RikWgkwsdo1B7lX259kHA1Esggb8Emcj6M9UUrrGVJVzV9ZWbKU3 N8e4X8wmPLYUY4/ MwYBY2Qs3e621PfMyzfa3xazaXa9yygSaR2LxmDlxgS5nJljoDRJoz1Fu81xT EI03JyjYEtQf4wsJrWVfni22HDZtloEgAoz9XCLJSk8IRGI07KIUteuJ+uOHgylp7YyLJ/MlbqoY 8VXDqHM8GpM= Fingerprint: 4e:05:7f:10:67:99:af:fb:0d:a2:79:a8:92:22:7e:48 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: aes256-

gcm@openssh.com chacha20-poly1305@openssh.com aes256-ctr aes256-cbc aes128-gcm@openssh.com aes128-ctr aes128-cbc MAC Algorithms: hmac-sha2-256-etm@openssh.com hmac-sha1-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha2-256 hmac-sha1 umac-128@openssh.com hmac-sha2-512 Compression Algorithms: none zlib@openssh.com ``` ---------- **443:** ``` ``` HEARTBLEED: 2023/08/30 23:02:53 45.154.12.151:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.154.12.151']

Name

proxy4.signalplus.org

Pattern Type

stix

Pattern

[hostname:value = 'proxy4.signalplus.org']

Name

http://flygram.org:4432

Pattern Type

stix

Pattern

[url:value = 'http://flygram.org:4432']

Name

proxy1.signalplus.org

Pattern Type

stix

Pattern

[hostname:value = 'proxy1.signalplus.org']

Name

proxy5.signalplus.org

Pattern Type

stix

Pattern

[hostname:value = 'proxy5.signalplus.org']

Name

flygram.org

Pattern Type

stix

Pattern

```
[domain-name:value = 'flygram.org']
```

Malware

Name
Uyghur Telegram
Name
BadBazaar
Name
GREF
Name
OS X
Name
FlyGram
Name
Android

Country

Name
Hungary
Name
Congo
Name
Denmark
Name
Yemen
Name
Portugal
Name
Lithuania
Name
Netherlands

Name
Singapore
Name
Spain
Name
Poland
Name
Hong Kong
Name
Brazil
Name
Australia
Name
China
Name
Germany
Name
United States of America

Name
Ukraine

Attack-Pattern

Name
Non-Standard Port
ID
T1509
Description
Adversaries may generate network traffic using a protocol and port paring that are typically not associated. For example, HTTPS over port 8088 or port 587 as opposed to the traditional port 443. Adversaries may make changes to the standard port used by a protocol to bypass filtering or muddle analysis/parsing of network data.
Name
Application Layer Protocol
ID
T1437
Description
Adversaries may communicate using application layer protocols to avoid detection/ network filtering by blending in with existing traffic. Commands to the mobile device, and often the results of those commands, will be embedded within the protocol traffic

between the mobile device and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS.

Name

Firmware Corruption

ID

T1495

Description

Adversaries may overwrite or corrupt the flash memory contents of system BIOS or other firmware in devices attached to a system in order to render them inoperable or unable to boot, thus denying the availability to use the devices and/or the system.(Citation: Symantec Chernobyl W95.CIH) Firmware is software that is loaded and executed from non-volatile memory on hardware devices in order to initialize and manage device functionality. These devices may include the motherboard, hard drive, or video cards. In general, adversaries may manipulate, overwrite, or corrupt firmware in order to deny the use of the system or devices. For example, corruption of firmware responsible for loading the operating system for network devices may render the network devices inoperable. (Citation: dhs_threat_to_net_devices)(Citation: cisa_malware_orgs_ukraine) Depending on the device, this attack may also result in [Data Destruction](https://attack.mitre.org/techniques/T1485).

Name

Data from Cloud Storage

ID

T1530

Description

Adversaries may access data from improperly secured cloud storage. Many cloud service providers offer solutions for online data object storage such as Amazon S3, Azure Storage,

and Google Cloud Storage. These solutions differ from other storage solutions (such as SQL or Elasticsearch) in that there is no overarching application. Data from these solutions can be retrieved directly using the cloud provider's APIs. In other cases, SaaS application providers such as Slack, Confluence, and Salesforce also provide cloud storage solutions as a peripheral use case of their platform. These cloud objects can be extracted directly from their associated application.(Citation: EA Hacked via Slack - June 2021)(Citation: SecureWorld - How Secure Is Your Slack Channel - Dec 2021)(Citation: HackerNews - 3 SaaS App Cyber Attacks - April 2022)(Citation: Dark Clouds_Usenix_Mulazzani_08_2011) Adversaries may collect sensitive data from these cloud storage solutions. Providers typically offer security guides to help end users configure systems, though misconfigurations are a common problem.(Citation: Amazon S3 Security, 2019)(Citation: Microsoft Azure Storage Security, 2019)(Citation: Google Cloud Storage Best Practices, 2019) There have been numerous incidents where cloud storage has been improperly secured, typically by unintentionally allowing public access to unauthenticated users, overly-broad access by all users, or even access for any anonymous person outside the control of the Identity Access Management system without even needing basic user permissions. This open access may expose various types of sensitive data, such as credit cards, personally identifiable information, or medical records.(Citation: Trend Micro S3 Exposed PII, 2017) (Citation: Wired Magecart S3 Buckets, 2019)(Citation: HIPAA Journal S3 Breach, 2017) (Citation: Rclone-mega-extortion_05_2021) Adversaries may also obtain then abuse leaked credentials from source repositories, logs, or other means as a way to gain access to cloud storage objects.

Name

Network Sniffing

ID

T1040

Description

Adversaries may sniff network traffic to capture information about an environment, including authentication material passed over the network. Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network, or use span ports to capture a larger amount of data. Data captured via this technique may include user credentials, especially those sent over an insecure, unencrypted protocol. Techniques for name service resolution poisoning, such as [LLMNR/NBT-NS Poisoning and SMB Relay]

(https://attack.mitre.org/techniques/T1557/001), can also be used to capture credentials to websites, proxies, and internal systems by redirecting traffic to an adversary. Network sniffing may also reveal configuration details, such as running services, version numbers, and other network characteristics (e.g. IP addresses, hostnames, VLAN IDs) necessary for subsequent Lateral Movement and/or Defense Evasion activities. In cloud-based environments, adversaries may still be able to use traffic mirroring services to sniff network traffic from virtual machines. For example, AWS Traffic Mirroring, GCP Packet Mirroring, and Azure vTap allow users to define specified instances to collect traffic from and specified targets to send collected traffic to.(Citation: AWS Traffic Mirroring)(Citation: GCP Packet Mirroring)(Citation: Azure Virtual Network TAP) Often, much of this traffic will be in cleartext due to the use of TLS termination at the load balancer level to reduce the strain of encrypting and decrypting traffic.(Citation: Rhino Security Labs AWS VPC Traffic Mirroring)(Citation: SpecterOps AWS Traffic Mirroring) The adversary can then use exfiltration techniques such as Transfer Data to Cloud Account in order to access the sniffed traffic.(Citation: Rhino Security Labs AWS VPC Traffic Mirroring) On network devices, adversaries may perform network captures using [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `monitor capture`.(Citation: US-CERT-TA18-106A)(Citation: capture_embedded_packet_on_software)

Name

System Network Configuration Discovery

ID

T1422

Description

Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of operating systems they access or through information discovery of remote systems. On Android, details of onboard network interfaces are accessible to apps through the `java.net.NetworkInterface` class.(Citation: NetworkInterface) Previously, the Android `TelephonyManager` class could be used to gather telephony-related device identifiers, information such as the IMSI, IMEI, and phone number. However, starting with Android 10, only preloaded, carrier, the default SMS, or device and profile owner applications can access the telephony-related device identifiers.(Citation: TelephonyManager) On iOS, gathering network configuration information is not possible without root access. Adversaries may use the information from [System Network Configuration Discovery](https://attack.mitre.org/techniques/T1422) during automated

discovery to shape follow-on behaviors, including determining certain access within the target network and what actions to do next.

Name

Software Discovery

ID

T1418

Description

Adversaries may attempt to get a listing of applications that are installed on a device. Adversaries may use the information from [Software Discovery](https://attack.mitre.org/techniques/T1418) during automated discovery to shape follow-on behaviors, including whether or not to fully infect the target and/or attempts specific actions. Adversaries may attempt to enumerate applications for a variety of reasons, such as figuring out what security measures are present or to identify the presence of target applications.

Name

Data from Local System

ID

T1533

Description

Adversaries may search local system sources, such as file systems or local databases, to find files of interest and sensitive data prior to exfiltration. Access to local system data, which includes information stored by the operating system, often requires escalated privileges. Examples of local system data include authentication tokens, the device keyboard cache, Wi-Fi passwords, and photos. On Android, adversaries may also attempt to access files from external storage which may require additional storage-related permissions.

Name

Location Tracking

ID

T1430

Description

Adversaries may track a device's physical location through use of standard operating system APIs via malicious or exploited applications on the compromised device. On Android, applications holding the `ACCESS_COAURSE_LOCATION` or `ACCESS_FINE_LOCATION` permissions provide access to the device's physical location. On Android 10 and up, declaration of the `ACCESS_BACKGROUND_LOCATION` permission in an application's manifest will allow applications to request location access even when the application is running in the background.(Citation: Android Request Location Permissions) Some adversaries have utilized integration of Baidu map services to retrieve geographical location once the location access permissions had been obtained.(Citation: PaloAlto-SpyDealer)(Citation: Palo Alto HenBox) On iOS, applications must include the `NSLocationWhenInUseUsageDescription`, `NSLocationAlwaysAndWhenInUseUsageDescription`, and/or `NSLocationAlwaysUsageDescription` keys in their `Info.plist` file depending on the extent of requested access to location information.(Citation: Apple Requesting Authorization for Location Services) On iOS 8.0 and up, applications call `requestWhenInUseAuthorization()` to request access to location information when the application is in use or `requestAlwaysAuthorization()` to request access to location information regardless of whether the application is in use. With elevated privileges, an adversary may be able to access location data without explicit user consent with the `com.apple.locationd.preauthorized` entitlement key.(Citation: Google Project Zero Insomnia)

Name

System Information Discovery

ID

T1426

Description

Adversaries may attempt to get detailed information about a device's operating system and hardware, including versions, patches, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1426) during automated discovery to shape follow-on behaviors, including whether or not to fully infects the target and/or attempts specific actions. On Android, much of this information is programmatically accessible to applications through the `android.os.Build` class. (Citation: Android-Build) iOS is much more restrictive with what information is visible to applications. Typically, applications will only be able to query the device model and which version of iOS it is running.

Name

Proxy

ID

T1090

Description

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](https://attack.mitre.org/software/S0040), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

Name

Access Token Manipulation

ID

T1134

Description

Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access tokens to determine the ownership of a running process. A user can manipulate access tokens to make a running process appear as though it is the child of a different process or belongs to someone other than the user that started the process. When this occurs, the process also takes on the security context associated with the new token. An adversary can use built-in Windows API functions to copy access tokens from existing processes; this is known as token stealing. These token can then be applied to an existing process (i.e. [Token Impersonation/Theft](https://attack.mitre.org/techniques/T1134/001)) or used to spawn a new process (i.e. [Create Process with Token](https://attack.mitre.org/techniques/T1134/002)). An adversary must already be in a privileged user context (i.e. administrator) to steal a token. However, adversaries commonly use token stealing to elevate their security context from the administrator level to the SYSTEM level. An adversary can then use a token to authenticate to a remote system as the account for that token if the account has appropriate permissions on the remote system.(Citation: Pentestlab Token Manipulation) Any standard user can use the `runas` command, and the Windows API functions, to create impersonation tokens; it does not require access to an administrator account. There are also other mechanisms, such as Active Directory fields, that can be used to modify access tokens.

Name

Application Layer Protocol

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Name

System Information Discovery

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

Intrusion-Set

Name
Ke3chang

Description
[Ke3chang](https://attack.mitre.org/groups/G0004) is a threat group attributed to actors operating out of China. [Ke3chang](https://attack.mitre.org/groups/G0004) has targeted oil, government, diplomatic, military, and NGOs in Central and South America, the Caribbean, Europe, and North America since at least 2010.(Citation: Mandiant Operation Ke3chang November 2014)(Citation: NCC Group APT15 Alive and Strong)(Citation: APT15 Intezer June 2018)(Citation: Microsoft NICKEL December 2021)

Domain-Name

Value
signalplus.org
vultrusercontent.com
flygram.org

StixFile

Value
3460330f4187163e2f0ee96c034a2db3c386de3dff5a8b6c8180ab3260bc705b

Hostname

Value
www.signalplus.org
proxy6.signalplus.org
proxy1.signalplus.org
proxy4.signalplus.org
www.flygram.org
mail.pmumail.com
proxy5.signalplus.org
45.63.89.238.vultrusercontent.com
proxy3.signalplus.org
proxy2.signalplus.org

IPv4-Addr

Value
148.251.87.245
45.154.12.151
82.180.174.230
103.27.186.195
185.239.227.14
154.202.59.169
92.118.189.164
45.154.12.202
45.63.89.238
103.27.186.156
217.163.29.84
45.133.238.92
45.154.12.132

156.67.73.71

Url

Value
http://flygram.org:4432
http://vultrusercontent.com
http://signalplus.org:4332

External References

- https://otx.alienvault.com/pulse/64f09f67430167a084c508ac
- https://www.welivesecurity.com/en/eset-research/badbazaar-espionage-tool-targets-android-users-trojanized-signal-telegram-apps/