Apr 08 2024

NETMANAGEIT

Intelligence Report

The Latest MuddyWater Attack Framework

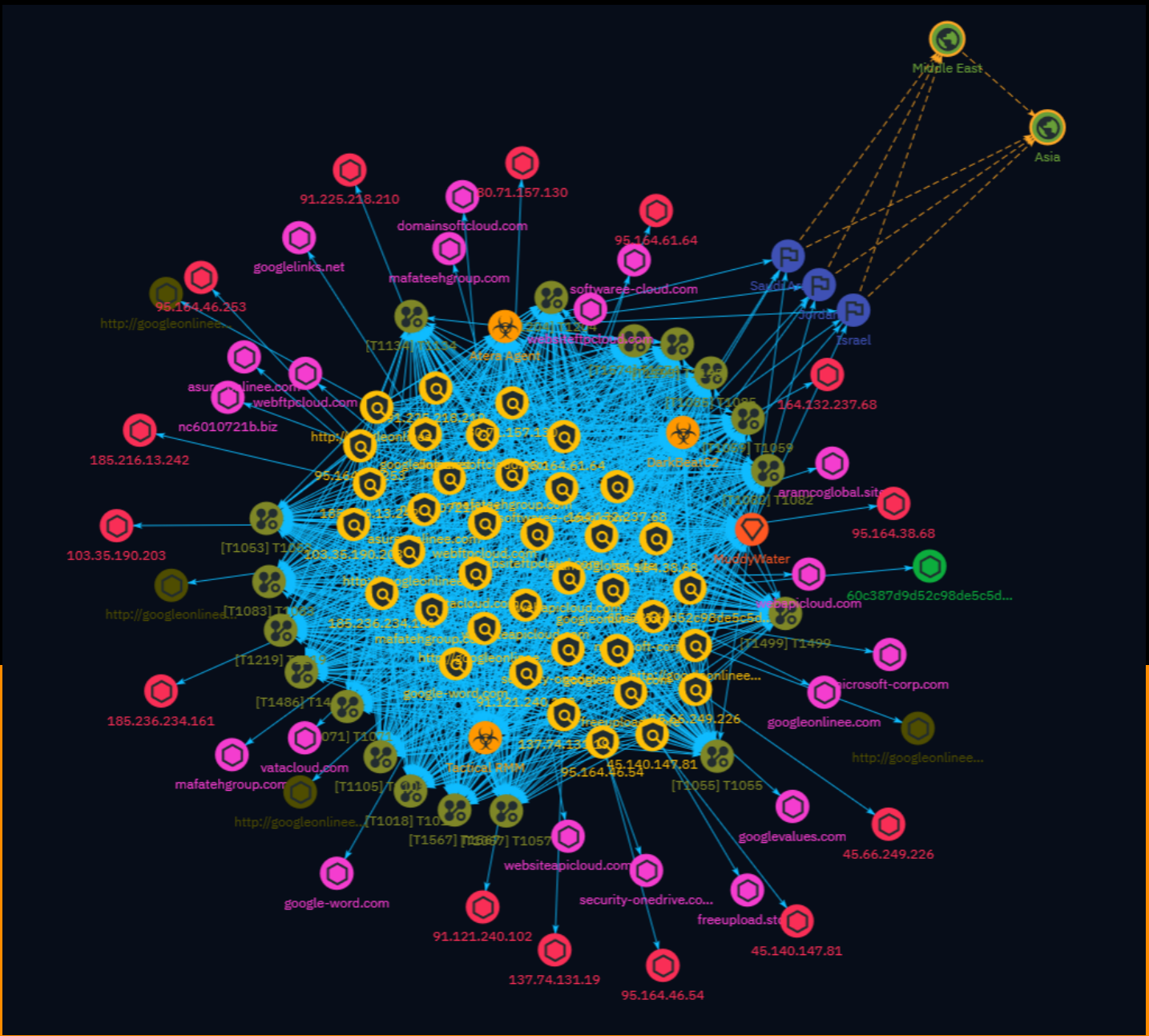

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The post details the latest malicious activities of the Iranian threat actor group MuddyWater, also known as MERCURY. It sheds light on their evolving tactics and the introduction of a new command and control (C2) framework dubbed 'DarkBeatC2'. The report provides analysis of the group's recent campaigns, supply chain attacks, and their potential collaboration with other Iranian groups. It also explores their abuse of compromised accounts and infrastructure to conduct phishing attacks and deploy remote access tools (RATs) against Israeli organizations.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

websiteftpcloud.com

Description

- **Unsafe:** False - **Server:** Apache/2.4.52 (Ubu - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1701160474, 'iso': '2023-11-28T03:34:34-05:00'} - **IPQS: Domain:** websiteftpcloud.com - **IPQS: IP Address:** 91.225.218.210

Pattern Type

stix

Pattern

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

Name

websiteapicloud.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4

months ago', 'timestamp': 1701160475, 'iso': '2023-11-28T03:34:35-05:00'} - **IPQS: Domain:** websiteapicloud.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

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

Name

webftpcloud.com

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': '6 months ago', 'timestamp': 1697953238, 'iso': '2023-10-22T01:40:38-04:00'} - **IPQS: Domain:** webftpcloud.com - **IPQS: IP Address:** 95.164.46.54

Pattern Type

stix

Pattern

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

Name

webapicloud.com

Description

- **Unsafe:** False - **Server:** Apache/2.4.52 (Ubu - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '6 months ago', 'timestamp': 1697953227, 'iso': '2023-10-22T01:40:27-04:00'} - **IPQS: Domain:** webapicloud.com - **IPQS: IP Address:** 95.164.61.64

Pattern Type

stix

Pattern

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

Name

vatacloud.com

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Malicious websites - **Domain Age:** {'human': '2 months ago', 'timestamp': 1706728948, 'iso': '2024-01-31T14:22:28-05:00'} - **IPQS: Domain:** vatacloud.com - **IPQS: IP Address:** 204.11.56.48

Pattern Type

stix

Pattern

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

Name

softwaree-cloud.com

Description

- **Unsafe:** False - **Server:** Apache/2.4.52 (Ubu - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '6 months ago', 'timestamp': 1697953249, 'iso': '2023-10-22T01:40:49-04:00'} - **IPQS: Domain:** softwaree-cloud.com - **IPQS: IP Address:** 95.164.38.68

Pattern Type

stix

Pattern

[domain-name:value = 'softwaree-cloud.com']

Name

security-onedrive.com

Description

- **Unsafe:** True - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '6 months ago', 'timestamp': 1695661316, 'iso': '2023-09-25T13:01:56-04:00'} - **IPQS: Domain:** security-onedrive.com - **IPQS: IP Address:** 15.197.130.221

Pattern Type

stix

Pattern

[domain-name:value = 'security-onedrive.com']

Name

nc6010721b.biz

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 minute ago', 'timestamp': 1712575639, 'iso': '2024-04-08T07:27:19-04:00'} - **IPQS: Domain:** nc6010721b.biz - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'nc6010721b.biz']

Name

microsoft-corp.com

Description

- **Unsafe:** True - **Server:** Apache/2.4.52 (Ubu - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 years ago', 'timestamp': 1646294151, 'iso': '2022-03-03T02:55:51-05:00'} - **IPQS: Domain:** microsoft-corp.com - **IPQS: IP Address:** 80.71.157.130

Pattern Type

stix

Pattern

[domain-name:value = 'microsoft-corp.com']

Name

mafatehgroup.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '7 months ago', 'timestamp': 1694932566, 'iso': '2023-09-17T02:36:06-04:00'} - **IPQS: Domain:** mafatehgroup.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

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

Name

mafateehgroup.com

Description

- **Unsafe:** False - **Server:** Apache - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3

years ago', 'timestamp': 1631705614, 'iso': '2021-09-15T07:33:34-04:00'} - **IPQS: Domain:** mafateehgroup.com - **IPQS: IP Address:** 92.205.5.35

Pattern Type

stix

Pattern

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

Name

googlevalues.com

Description

- **Unsafe:** False - **Server:** Apache/2.4.41 (Ubu - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1707625876, 'iso': '2024-02-10T23:31:16-05:00'} - **IPQS: Domain:** googlevalues.com - **IPQS: IP Address:** 137.74.131.19

Pattern Type

stix

Pattern

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

Name

googlelinks.net

Description

- **Unsafe:** False - **Server:** Apache/2.4.41 (Ubu - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1707625868, 'iso': '2024-02-10T23:31:08-05:00'} - **IPQS: Domain:** googlelinks.net - **IPQS: IP Address:** 91.121.240.102

Pattern Type

stix

Pattern

[domain-name:value = 'googlelinks.net']

Name

googleonlinee.com

Description

- **Unsafe:** True - **Server:** Apache/2.4.52 (Ubu - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1701160389, 'iso': '2023-11-28T03:33:09-05:00'} - **IPQS: Domain:** googleonlinee.com - **IPQS: IP Address:** 95.164.46.253

Pattern Type

stix

Pattern

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

Name

google-word.com

Description

- **Unsafe:** False - **Server:** Apache/2.4.41 (Ubu - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1707625860, 'iso': '2024-02-10T23:31:00-05:00'} - **IPQS: Domain:** google-word.com - **IPQS: IP Address:** 164.132.237.68

Pattern Type

stix

Pattern

[domain-name:value = 'google-word.com']

Name

domainsoftcloud.com

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1707950390, 'iso': '2024-02-14T17:39:50-05:00'} - **IPQS: Domain:** domainsoftcloud.com - **IPQS: IP Address:** 45.140.147.81

Pattern Type

stix

Pattern

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

Name

freeupload.store

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '10 months ago', 'timestamp': 1685979389, 'iso': '2023-06-05T11:36:29-04:00'} - **IPQS: Domain:** freeupload.store - **IPQS: IP Address:** 51.255.19.181

Pattern Type

stix

Pattern

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

Name

asure-onlinee.com

Description

- **Unsafe:** True - **Server:** Apache/2.4.52 (Ubu - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1701093388, 'iso': '2023-11-27T08:56:28-05:00'} - **IPQS: Domain:** asure-onlinee.com - **IPQS: IP Address:** 103.35.190.203

Pattern Type

stix

Pattern

[domain-name:value = 'asure-onlinee.com']

Name

aramcoglobal.site

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': '4 months ago', 'timestamp': 1702929888, 'iso': '2023-12-18T15:04:48-05:00'} - **IPQS: Domain:** aramcoglobal.site - **IPQS: IP Address:** 185.236.234.161

Pattern Type

stix

Pattern

[domain-name:value = 'aramcoglobal.site']

Name

http://googleonlinee.com/zero/8946172/eUwYPH9eIbAOiLs

Description

- **Unsafe:** True - **Server:** Apache/2.4.52 (Ubu - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4

months ago', 'timestamp': 1701160389, 'iso': '2023-11-28T03:33:09-05:00'} - **IPQS: Domain:** googleonlinee.com - **IPQS: IP Address:** 95.164.46.253

Pattern Type

stix

Pattern

[url:value = 'http://googleonlinee.com/zero/8946172/eUwYPH9eIbAOiLs']

Name

http://googleonlinee.com/zero/8946172/0IGkmSybmd3BXIe

Description

- **Unsafe:** True - **Server:** Apache/2.4.52 (Ubu - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1701160389, 'iso': '2023-11-28T03:33:09-05:00'} - **IPQS: Domain:** googleonlinee.com - **IPQS: IP Address:** 95.164.46.253

Pattern Type

stix

Pattern

[url:value = 'http://googleonlinee.com/zero/8946172/0IGkmSybmd3BXIe']

Name

http://googleonlinee.com/zero/7878123/eUwYPH9eIbAOiLs

Description

- **Unsafe:** True - **Server:** Apache/2.4.52 (Ubu - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1701160389, 'iso': '2023-11-28T03:33:09-05:00'} - **IPQS: Domain:** googleonlinee.com - **IPQS: IP Address:** 95.164.46.253

Pattern Type

stix

Pattern

[url:value = 'http://googleonlinee.com/zero/7878123/eUwYPH9eIbAOiLs']

Name

http://googleonlinee.com/setting/8955224/r4WB7DzDOwfaHSevxHH0

Description

- **Unsafe:** True - **Server:** Apache/2.4.52 (Ubu - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1701160389, 'iso': '2023-11-28T03:33:09-05:00'} - **IPQS: Domain:** googleonlinee.com - **IPQS: IP Address:** 95.164.46.253

Pattern Type

stix

Pattern

[url:value = 'http://googleonlinee.com/setting/8955224/r4WB7DzDOwfaHSevxHH0']

Name

95.164.61.64

Description

ISP: STARK INDUSTRIES SOLUTIONS LTD **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBK/YivnxwmEhCTHPPdOlozJK tfyisUD074XSuGDkK0h+KXORGLVdlOpAV+C1MLJHUD+cEw6T/BzPQRmatrGoZ/w= Fingerprint: f9:bd:d0:ec:dd:76:22:8d:22:8f:26:c4:29:2a:71:ff 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 kex-strict-s-v00@openssh.com 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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Mon, 25 Mar 2024 12:52:52 GMT Server: Apache/2.4.52 (Ubuntu) Last-Modified: Wed, 08 Nov 2023 08:15:25 GMT ETag: "b0-6099fb07a6835" Accept-Ranges: bytes Content-Length: 176 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **443:** ``` HTTP/1.1 200 OK Date: Wed, 03 Apr 2024 16:47:25 GMT Server: Apache/2.4.52 (Ubuntu) Last-Modified: Wed, 08 Nov 2023 08:15:25 GMT ETag: "b0-6099fb07a6835" Accept-Ranges: bytes Content-Length: 176 Vary: Accept-Encoding Content-Type: text/html ``` HEARTBLEED: 2024/04/03 16:47:40 95.164.61.64:443 - SAFE ---------- **8008:** ``` HTTP/1.1 200 OK Content-Type: text/html; charset=utf-8 Content-Length: 3220 Last-Modified: Tue, 10 Oct 2023 13:31:00 GMT Cache-Control: private, must-revalidate Pragma: private Server: SimpleHelp/SSuite-5-4-20231010-143523 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '95.164.61.64']

Name

95.164.46.54

Description

ISP: STARK INDUSTRIES SOLUTIONS LTD **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMxTgXe+DjMDsXcXg2JxRIKA fN+ksVaNr7gcWt4XAdPePS72TeGj5agBgyfUsfhDC7NQXDAmDBY7cg565H49+2M= Fingerprint: df:f6:67:9c:1f:79:1f:c1:76:2a:b5:11:af:c0:87:57 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 kex-strict-s-v00@openssh.com 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 = '95.164.46.54']

Name

95.164.46.253

Description

ISP: STARK INDUSTRIES SOLUTIONS LTD **OS:** - ---------- Services: **80:** ``` HTTP/1.1 200 OK Date: Fri, 05 Apr 2024 10:43:19 GMT Server: Apache/2.4.52 (Ubuntu) Last-Modified: Sat, 13 Jan 2024 09:19:44 GMT ETag: "b7-60ed04803e59d" Accept-Ranges: bytes Content-Length: 183 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Date: Wed, 20 Mar 2024 00:53:47 GMT Server: Apache/2.4.52 (Ubuntu) Content-Type: text/plain; charset=utf-8 X-Content-Type-Options: nosniff Content-Length: 19 ``` HEARTBLEED: 2024/03/20 00:54:02 95.164.46.253:443 - SAFE ---------- **8000:** ``` HTTP/1.1 403 Forbidden Content-Type: text/plain; charset=utf-8 X-Content-Type-Options: nosniff Date: Mon, 08 Apr 2024 09:29:12 GMT Content-Length: 10 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '95.164.46.253']

Name

95.164.38.68

Description

ISP: STARK INDUSTRIES SOLUTIONS LTD **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGgFIkA89Afq7GTLXgDGB8LCujhDO5DcsBCd6ZWDnGJxL39E8RFWuqmFruUzZo2cuJpoHHRyrHRT4+MpK7vwjBI= Fingerprint: fd:77:0e:76:86:dd:ea:5c:df:f5:02:87:ab:f3:57:97 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 kex-strict-s-v00@openssh.com 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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Sat, 16 Mar 2024 13:36:07 GMT Server: Apache/2.4.52 (Ubuntu) Last-Modified: Sat, 13 Jan 2024 12:08:12 GMT ETag: "b0-60ed2a27e0352" Accept-Ranges: bytes Content-Length: 176 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **443:** ``` HTTP/1.1 200 OK Date: Fri, 05 Apr 2024 07:09:27 GMT Server: Apache/2.4.52 (Ubuntu) Last-Modified: Sat, 13 Jan 2024 12:08:12 GMT ETag: "b0-60ed2a27e0352" Accept-Ranges: bytes Content-Length: 176 Vary: Accept-Encoding Content-Type: text/html ``` HEARTBLEED: 2024/04/05 07:09:37 95.164.38.68:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '95.164.38.68']

Name

91.121.240.102

Description

ISP: OVH SAS **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.2 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDSX1h6LM/9Zefjt0ozGAaAteduEpRd9ve/NBKE7TwuP0Hq D2n3cZYagvGtx7lEXRIlpgOKVRE26RejOQP8n6qOlZw8mRVOn1/9xI/JZyfTbgqq74ZujWQehzBa UhI4A6Q/RxMDYdOGGlI257DPXPaM9oK0jRs562I7B5qHq+g+DZpWYUYkT88dm/OkK2ip/GO9pwEg ZLysXj7d/nV+o67YFsVZNRESiR3jvY4o/M9rEFBxofcroyIFaYTjrjrL9XFokcWHtAisA7luy7WL kCK7hfFAiKB9W9h9rF58fuom/h2nNt76cGZ8ykoHvLkq+UmJ8JXHlR+EA6vcfJ1Zp7MtJd2vgUfq bI1q4gBiGRLLsUC6MtHZsqH7tiOQE6SEEIITgDK3KU5pGPq6kSVlZkaAg/itChCktbQBbd8ZYe57 TMKZAeJoBSr7FB2r6RldOqlSc3asMC9+A07ZZJjgMSuUBOJzUmobJrA33jTg/aQJx196MrHLwiCm WlSWRNNM4tc= Fingerprint: 92:b3:da:ae:bd:17:18:f9:2a:24:8b:47:6a:a6:82:94 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 Date: Thu, 04 Apr 2024 21:09:23 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Mon, 12 Feb 2024 15:26:51 GMT ETag: "b0-61130e82b78a0" Accept-Ranges: bytes Content-Length: 176 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Date: Sun, 31 Mar 2024 13:12:22 GMT Server: Apache/2.4.41 (Ubuntu) Content-Type: text/plain; charset=utf-8 X-Content-Type-Options: nosniff Content-Length: 19 ``` HEARTBLEED: 2024/03/31 13:12:41 91.121.240.102:443 - SAFE ---------- **8000:** ``` HTTP/1.1 404 Not Found Content-Type: text/plain; charset=utf-8 X-Content-Type-Options: nosniff Date: Tue, 26 Mar 2024 02:48:25 GMT Content-Length: 19 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.121.240.102']

Name

91.225.218.210

Description

ISP: STARK INDUSTRIES SOLUTIONS LTD **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKnDfcA3ziZ4Fbo0cA0gNqF4MkjxP6go0zZBxu1nq+L5Txx30P240z9WwgWyAsLcNArBEx4JieTO9+2Nfo+Ym0Y= Fingerprint: 9c:01:c6:cd:6b:f1:d7:e5:89:60:72:54:e2:37:af:ea 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 kex-strict-s-v00@openssh.com 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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Wed, 27 Mar 2024 22:23:07 GMT Server: Apache/2.4.52 (Ubuntu) Last-Modified: Wed, 06 Dec 2023 05:08:38 GMT ETag: "b0-60bd058056c8b" Accept-Ranges: bytes Content-Length: 176 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **443:** ``` HTTP/1.1 503 Service Unavailable Date: Fri, 29 Mar 2024 09:37:08 GMT Server: Apache/2.4.52 (Ubuntu) Content-Length: 380 Connection: close Content-Type: text/html; charset=iso-8859-1 ``` HEARTBLEED: 2024/03/29 09:37:21 91.225.218.210:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.225.218.210']

Name

45.66.249.226

Description

ISP: BlueVPS OU **OS:** - ---------- Services: **443:** ``` HTTP/1.1 200 OK Server: nginx Date: Wed, 03 Apr 2024 15:28:28 GMT Content-Type: text/html; charset=utf-8 Content-Length: 628 Last-Modified: Sat, 03 Feb 2024 01:46:16 GMT Connection: keep-alive ETag: "65bd9ae8-274" Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Accept-Ranges: bytes ``` HEARTBLEED: 2024/04/03 15:28:54 45.66.249.226:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.66.249.226']

Name

185.216.13.242

Description

ISP: STARK INDUSTRIES SOLUTIONS LTD **OS:** - ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Fri, 05 Apr 2024 03:00:16 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Tue, 11 Apr 2023 01:45:34 GMT Connection: keep-alive ETag: "6434bbbe-267" Accept-Ranges: bytes ``` ---------- **443:** ``` HTTP/1.1 400 Bad Request Server: nginx Date: Fri, 05 Apr 2024 20:05:05 GMT Content-Type: text/html; charset=utf-8 Content-Length: 650 Connection: close ``` ---------- **1024:** ``` HTTP/1.1 302 Found strict-transport-security: max-age=60000; includeSubDomains Referrer-Policy: no-referrer x-frame-options: SAMEORIGIN X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Content-Security-Policy: default-src 'none'; style-src 'self' 'unsafe-inline'; Location: https://185.216.13.242:443/ Vary: Accept Content-Type: text/html; charset=utf-8 Content-Length: 98 Date: Fri, 05 Apr 2024 20:05:03 GMT Connection: keep-alive Keep-Alive: timeout=5 ``` ---------- **4369:** ``` Erlang Port Mapper Daemon: nodes: rabbit: 25672 ``` ---------- **4430:** ``` HTTP/1.1 200 OK Referrer-Policy: no-referrer X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Content-Security-Policy: default-src 'none'; font-src 'self'; script-src 'self' 'unsafe-inline'; connect-src 'self' *.openstreetmap.org wss://185.216.13.242; img-src 'self' blob: data: *.openstreetmap.org data:; style-src 'self' 'unsafe-inline'; frame-src 'self' mcrouter:; media-src 'self'; form-action 'self' Permissions-Policy: interest-cohort=() Strict-Transport-Security: max-age=63072000 Cache-Control: no-store Content-Type: text/html; charset=utf-8 Content-Length: 66378 ETag: W/"1034a-ro5zfJADlh31O7lHDWxLPtMoT9c" Vary: Accept-Encoding Date: Fri, 15 Mar 2024 01:00:09 GMT Connection: keep-alive Keep-Alive: timeout=5 ``` ---------- **5672:** ``` AMQP: Protocol Version: 0-9 Product: RabbitMQ Product Version: 3.13.0 Platform: Erlang/OTP 26.2.2 Capabilities: Exchange Exchange Bindings: True Connection.blocked: True Authentication Failure Close: True Direct Reply To: True Basic.nack: True Per Consumer Qos: True Consumer Priorities: True Consumer Cancel Notify: True Publisher Confirms: True ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.216.13.242']

Name

164.132.237.68

Description

ISP: OVH SAS **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.2 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDeHuymMsicVTmPElcaDjT+5GTsdS4PtKOAjEi9FymoaSBn iFTUSdKNpm1JRxHkv/8XwryaSgnI/eSisq1ujL5Rk94w+pDLacFrbUkCdEjqPDgn7PcyQGYoSg+Fut9Sf5gXeNhInICORNGrwQryrkLexF34gU8NYFwS9CgHECfRs+TzDV95udE1Ik++t8xFi9lrBQ+QPc2NgJPh2B0/w/VX7lDMrIa1V3AykfEHgZ0X0rxqU4oRQbGk2EaAFgNYk2Te+MdsRTcG8+MOQNDN0z6cFK1DZKEMDHvBLiAndv8+rEBsoY0/GHnntTGE+BcEQb1Lo3MDh/ysTZDGSc0LFTTZ9zPnayKFjumQDIM8aK1I/kzP4yKNakgg6IZSKK5isV8y4g4mtIKKZI8VCdTAF4iXxZjU10eTujh53FRZKz7DmQT5hw/4YD8DzkY0uF3RMrTmwSip5bzVR5HUZWoROptB54z71XyZHOtSNgAj0uFOYtLkkxMyI5V0E8MJTSLVFzE= Fingerprint: f3:1a:8b:47:09:4c:c0:1a:ed:28:1c:a1:47:45:9c:c8 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 Date: Fri, 05 Apr 2024 21:11:15 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Mon, 12 Feb 2024 07:24:00 GMT ETag: "b0-6112a2955db1f" Accept-Ranges: bytes Content-Length: 176 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Date: Mon, 01 Apr 2024 04:59:32 GMT Server: Apache/2.4.41 (Ubuntu) Content-Type: text/plain; charset=utf-8 X-Content-Type-Options: nosniff Content-Length: 19 ``` HEARTBLEED: 2024/04/01 05:00:03 164.132.237.68:443 - SAFE ---------- **8000:** ```

HTTP/1.1 403 Forbidden Content-Type: text/plain; charset=utf-8 X-Content-Type-Options: nosniff Date: Wed, 03 Apr 2024 22:20:02 GMT Content-Length: 10 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '164.132.237.68']

Name

137.74.131.19

Description

ISP: OVH SAS **OS:** - ---------- Services: **80:** ``` HTTP/1.1 200 OK Date: Fri, 05 Apr 2024 21:47:45 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Mon, 12 Feb 2024 08:42:34 GMT ETag: "b0-6112b4257d38c" Accept-Ranges: bytes Content-Length: 176 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Date: Wed, 03 Apr 2024 05:43:05 GMT Server: Apache/2.4.41 (Ubuntu) Content-Type: text/plain; charset=utf-8 X-Content-Type-Options: nosniff Content-Length: 19 ``` HEARTBLEED: 2024/04/03 05:43:15 137.74.131.19:443 - SAFE ---------- **8000:** ``` HTTP/1.1 403 Forbidden Content-Type: text/plain; charset=utf-8 X-Content-Type-Options: nosniff Date: Wed, 03 Apr 2024 05:30:57 GMT Content-Length: 10 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '137.74.131.19']

Name

103.35.190.203

Description

ISP: STARK INDUSTRIES SOLUTIONS LTD **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAWw4xNwsYHaReBIglDyp Hix 8Mq/s2V+SU4Gdc5d4NWgqiV1VlrqoIqBEyxCHAOc2A0o3/gX5xQUiuWvfQSjzaU= Fingerprint: 09:3d:a3:51:90:91:67:7a:a3:a5:ef:5b:b7:ba:f1:30 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 kex-strict-s-v00@openssh.com 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 ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Mon, 25 Mar 2024 09:58:59 GMT Server: Apache/2.4.52 (Ubuntu) Last-Modified: Sat, 13 Jan 2024 10:51:14 GMT ETag: "b7-60ed18f3e9b4a" Accept-Ranges: bytes Content-Length: 183 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Date: Mon, 01 Apr 2024 04:27:05 GMT Server: Apache/2.4.52 (Ubuntu) Content-Type: text/plain; charset=utf-8 X-Content-Type-Options: nosniff Content-Length: 19 ``` HEARTBLEED: 2024/04/01 04:27:23 103.35.190.203:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.35.190.203']

Name

60c387d9d52c98de5c5d8453f64a6541ec4db645f6709d1fe51903182943438c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '60c387d9d52c98de5c5d8453f64a6541ec4db645f6709d1fe51903182943438c']

Name

185.236.234.161

Description

ISP: STARK INDUSTRIES SOLUTIONS LTD **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMWS6jVgkg4BIR7Bp8x5U4nq gdY5S4omIQBbQOe/h9Ab7q2vVpq/0VguOBLH4ST8Z7oPeuWqid5J/2v7LFrDzJw= Fingerprint: 18:29:d3:b5:90:ab:e5:4e:2a:57:d9:22:a0:b0:32:92 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 kex-strict-s-v00@openssh.com 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 ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Date: Wed, 27 Mar 2024 02:18:05 GMT Content-Length: 0 ``` HEARTBLEED: 2024/03/27 02:18:14 185.236.234.161:443 - SAFE ---------- **4443:** ``` HTTP/1.1 200 OK Server: nginx/1.25.4 Date: Thu, 04 Apr 2024 07:45:42 GMT Content-Type: text/html; charset=utf-8 Content-Length: 4516 Connection: keep-alive Expires: Thu, 04 Apr 2024 07:45:42 GMT Cache-Control: max-age=0, no-cache, no-store, must-revalidate, private Vary: Cookie X-Frame-Options: DENY X-Content-Type-Options: nosniff Referrer-Policy: same-origin Set-Cookie: csrftoken=kvy1Pn2jG2EZPsY2BSfpBYMwiXYkrZyp33anBhh1P8lkfXq0JNKx3cCdT0aUkL3l; expires=Thu, 03 Apr 2025 07:45:42 GMT; Max-Age=31449600; Path=/; SameSite=Lax ``` HEARTBLEED: 2024/04/04 07:45:52 185.236.234.161:4443 - SAFE ---------- **8000:** ```

HTTP/1.1 200 OK Date: Thu, 21 Mar 2024 23:30:30 GMT Server: WSGIServer/0.2 CPython/3.10.12 Content-Type: text/html; charset=utf-8 Expires: Thu, 21 Mar 2024 23:30:30 GMT Cache-Control: max-age=0, no-cache, no-store, must-revalidate, private Vary: Cookie X-Frame-Options: DENY Content-Length: 4516 X-Content-Type-Options: nosniff Referrer-Policy: same-origin Set-Cookie: csrftoken=aJp08h7A174ixEXqLtXV37troBdO6Omb372ZC6OwP7aJy2MjGjbW3kNHZ56lsv00; expires=Thu, 20 Mar 2025 23:30:30 GMT; Max-Age=31449600; Path=/; SameSite=Lax ``` ---------- **8082:** ``` HTTP/1.1 301 Moved Permanently Server: nginx/1.25.4 Date: Wed, 13 Mar 2024 19:50:56 GMT Content-Type: text/html Content-Length: 169 Connection: keep-alive Location: https://185.236.234.161/ ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.236.234.161']

Name

80.71.157.130

Description

ISP: STARK INDUSTRIES SOLUTIONS LTD **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEQzCHN7CHcCu8J5sd/FLvPe L+jFV8d1z7lhTq8UjKnNB32Z05HXCbcQxk9/RrGg79SRJWxdL08j81me67T+m3Q= Fingerprint: 7e:cc:f0:30:87:2a:d9:ef:56:c1:e3:8f:a6:e9:eb:65 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 kex-strict-s-v00@openssh.com 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 ```

---------- **80:** ``` HTTP/1.1 200 OK Date: Wed, 20 Mar 2024 14:56:55 GMT Server: Apache/2.4.52 (Ubuntu) Last-Modified: Sat, 13 Jan 2024 11:12:42 GMT ETag: "b7-60ed1dc02c970" Accept-Ranges: bytes Content-Length: 183 Vary: Accept-Encoding Content-Type: text/html ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Date: Wed, 13 Mar 2024 20:16:55 GMT Server: Apache/2.4.52 (Ubuntu) Content-Type: text/plain; charset=utf-8 X-Content-Type-Options: nosniff Content-Length: 19 ``` HEARTBLEED: 2024/03/13 20:17:30 80.71.157.130:443 - SAFE ---------- **8000:** ``` HTTP/1.1 403 Forbidden Content-Type: text/plain; charset=utf-8 X-Content-Type-Options: nosniff Date: Mon, 18 Mar 2024 23:35:22 GMT Content-Length: 10 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '80.71.157.130']

Name

45.140.147.81

Description

ISP: STARK INDUSTRIES SOLUTIONS LTD **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJHfAhVbQ6T28a+C2jNrcRqg h6u1rsgfg38MKN5i7Sjn5LsEoLISiJfuMvMqt8C9k8diwYsvcaw3K+ck3/T5FRE= Fingerprint: 00:28:ff:72:4b:22:48:f0:6f:da:cd:6e:81:1f:e3:c1 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 kex-strict-s-v00@openssh.com 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 ``` ---------- **443:** ``` HTTP/1.1 503 Service Unavailable Date: Sun, 10 Mar 2024 18:15:25

GMT Server: Apache/2.4.52 (Ubuntu) Content-Length: 379 Connection: close Content-Type: text/html; charset=iso-8859-1 ``` HEARTBLEED: 2024/03/10 18:15:32 45.140.147.81:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.140.147.81']

Malware

Name
DarkBeatC2
Name
Tactical RMM
Name
Atera Agent

Attack-Pattern

Name
T1085
ID
T1085
Name
T1018
ID
T1018
Description
Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as [Ping](https://attack.mitre.org/software/S0097) or `net view` using [Net](https://attack.mitre.org/software/S0039). Adversaries may also analyze data from local host files (ex: `C:\Windows\System32\Drivers\etc\hosts` or `/etc/hosts`) or other passive means (such as local [Arp](https://attack.mitre.org/software/S0099) cache entries) in order to discover the presence of remote systems in an environment. Adversaries may also target discovery of network infrastructure as well as leverage [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands on network devices to gather detailed information

about systems within a network (e.g. `show cdp neighbors`, `show arp`).(Citation: US-CERT-TA18-106A)(Citation: CISA AR21-126A FIVEHANDS May 2021)

Name

T1134

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

T1499

ID

T1499

Description

Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users. Endpoint DoS can be performed by exhausting the system resources those services are hosted on or exploiting the system to cause a persistent crash condition. Example services include websites, email services, DNS, and web-based applications. Adversaries have been observed conducting DoS attacks for political purposes(Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction(Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion.(Citation: Symantec DDoS October 2014) An Endpoint DoS denies the availability of a service without saturating the network used to provide access to the service. Adversaries can target various layers of the application stack that is hosted on the system used to provide the service. These layers include the Operating Systems (OS), server applications such as web servers, DNS servers, databases, and the (typically web-based) applications that sit on top of them. Attacking each layer requires different techniques that take advantage of bottlenecks that are unique to the respective components. A DoS attack may be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS). To perform DoS attacks against endpoint resources, several aspects apply to multiple methods, including IP address spoofing and botnets. Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices. Botnets are commonly used to conduct DDoS attacks against networks and services. Large botnets can generate a significant amount of traffic from systems spread across the global internet. Adversaries may have the resources to build out and control their own botnet infrastructure or may rent time on an existing botnet to conduct an attack. In some of the worst cases for DDoS, so many systems are used to generate requests that each one only needs to send out a small amount of traffic to produce enough volume to exhaust the target's resources. In such circumstances, distinguishing DDoS traffic from legitimate clients becomes exceedingly difficult. Botnets have been used in some of the most high-profile DDoS attacks, such as the 2012 series of incidents that targeted major US banks.(Citation: USNYAG IranianBotnet March 2016) In cases where traffic manipulation is used, there may be points in the global network (such as high traffic gateway routers) where packets can be altered and cause legitimate clients to execute code that directs network packets toward a target in high volume. This type of capability was previously used for the purposes of web censorship where client HTTP traffic was modified to include a reference to JavaScript that generated the DDoS code to overwhelm target web servers.(Citation: ArsTechnica Great Firewall of China) For attacks attempting to

saturate the providing network, see [Network Denial of Service](https://attack.mitre.org/techniques/T1498).

Name

T1486

ID

T1486

Description

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal Defacement](https://attack.mitre.org/techniques/T1491/001), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted.(Citation: Rhino S3 Ransomware Part 1)

Name

T1574

ID

T1574

Description

Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs. Hijacking execution flow can be for the purposes of persistence, since this hijacked execution may reoccur over time. Adversaries may also use these mechanisms to elevate privileges or evade defenses, such as application control or other restrictions on execution. There are many ways an adversary may hijack the flow of execution, including by manipulating how the operating system locates programs to be executed. How the operating system locates libraries to be used by a program can also be intercepted. Locations where the operating system looks for programs/resources, such as file directories and in the case of Windows the Registry, could also be poisoned to include malicious payloads.

Name

T1057

ID

T1057

Description

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. In Windows environments, adversaries could obtain details on running processes using the [Tasklist](https://attack.mitre.org/

software/S0057) utility via [cmd](https://attack.mitre.org/software/S0106) or `Get-Process` via [PowerShell](https://attack.mitre.org/techniques/T1059/001). Information about processes can also be extracted from the output of [Native API](https://attack.mitre.org/techniques/T1106) calls such as `CreateToolhelp32Snapshot`. In Mac and Linux, this is accomplished with the `ps` command. Adversaries may also opt to enumerate processes via /proc. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show processes` can be used to display current running processes.(Citation: US-CERT-TA18-106A)(Citation: show_processes_cisco_cmd)

Name

T1083

ID

T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A)

Name

T1059

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

T1105

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/

techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Name

T1204

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to

deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

T1055

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

T1219

ID

T1219

Description

An adversary may use legitimate desktop support and remote access software to establish an interactive command and control channel to target systems within networks. These services, such as `VNC`, `Team Viewer`, `AnyDesk`, `ScreenConnect`, `LogMein`,

`AmmyyAdmin`, and other remote monitoring and management (RMM) tools, are commonly used as legitimate technical support software and may be allowed by application control within a target environment.(Citation: Symantec Living off the Land)(Citation: CrowdStrike 2015 Global Threat Report)(Citation: CrySyS Blog TeamSpy) Remote access software may be installed and used post-compromise as an alternate communications channel for redundant access or as a way to establish an interactive remote desktop session with the target system. They may also be used as a component of malware to establish a reverse connection or back-connect to a service or adversary controlled system. Adversaries may similarly abuse response features included in EDR and other defensive tools that enable remote access. Installation of many remote access software may also include persistence (e.g., the software's installation routine creates a [Windows Service](https://attack.mitre.org/techniques/T1543/003)).

Name

T1195

ID

T1195

Description

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including: * Manipulation of development tools * Manipulation of a development environment * Manipulation of source code repositories (public or private) * Manipulation of source code in open-source dependencies * Manipulation of software update/distribution mechanisms * Compromised/infected system images (multiple cases of removable media infected at the factory)(Citation: IBM Storwize)(Citation: Schneider Electric USB Malware) * Replacement of legitimate software with modified versions * Sales of modified/counterfeit products to legitimate distributors * Shipment interdiction While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.(Citation: Avast CCleaner3 2018)(Citation: Microsoft Dofoil 2018)(Citation: Command Five SK 2011) Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Symantec Elderwood Sept 2012)(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011) Popular open source projects that are

used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

Name

T1567

ID

T1567

Description

Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to compromise. Firewall rules may also already exist to permit traffic to these services. Web service providers also commonly use SSL/TLS encryption, giving adversaries an added level of protection.

Name

T1053

ID

T1053

Description

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.(Citation: TechNet Task Scheduler Security) Adversaries may use task

scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process. (Citation: ProofPoint Serpent)

Name

T1082

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)

Name

T1071

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.

Intrusion-Set

Name

MuddyWater

Description

[MuddyWater](https://attack.mitre.org/groups/G0069) is a cyber espionage group assessed to be a subordinate element within Iran's Ministry of Intelligence and Security (MOIS). (Citation: CYBERCOM Iranian Intel Cyber January 2022) Since at least 2017, [MuddyWater] (https://attack.mitre.org/groups/G0069) has targeted a range of government and private organizations across sectors, including telecommunications, local government, defense, and oil and natural gas organizations, in the Middle East, Asia, Africa, Europe, and North America.(Citation: Unit 42 MuddyWater Nov 2017)(Citation: Symantec MuddyWater Dec 2018) (Citation: ClearSky MuddyWater Nov 2018)(Citation: ClearSky MuddyWater June 2019) (Citation: Reaqta MuddyWater November 2017)(Citation: DHS CISA AA22-055A MuddyWater February 2022)(Citation: Talos MuddyWater Jan 2022)

Country

Name
Saudi Arabia
Name
Jordan
Name
Israel

Region

Name
Middle East

Name
Asia

Domain-Name

Value
websiteftpcloud.com
websiteapicloud.com
webftpcloud.com
webapicloud.com
vatacloud.com
softwaree-cloud.com
security-onedrive.com
nc6010721b.biz
microsoft-corp.com
mafatehgroup.com
mafateehgroup.com
googlevalues.com
googleonlinee.com

googlelinks.net
google-word.com
freeupload.store
asure-onlinee.com
aramcoglobal.site
domainsoftcloud.com

Url

Value
http://googleonlinee.com/zero/8946172/eUwYPH9eIbAOiLs
http://googleonlinee.com/zero/7878123/eUwYPH9eIbAOiLs
http://googleonlinee.com/zero/8946172/0IGkmSybmd3BXIe
http://googleonlinee.com/setting/8955224/r4WB7DzDOwfaHSevxHH0

IPv4-Addr

Value
95.164.61.64
95.164.46.54
95.164.46.253
95.164.38.68
91.225.218.210
91.121.240.102
45.66.249.226
185.216.13.242
164.132.237.68
137.74.131.19
103.35.190.203
185.236.234.161
80.71.157.130

45.140.147.81

StixFile

Value
60c387d9d52c98de5c5d8453f64a6541ec4db645f6709d1fe51903182943438c

External References

- https://www.deepinstinct.com/blog/darkbeatc2-the-latest-muddywater-attack-framework
- https://otx.alienvault.com/pulse/6613d03e774c84592c8233ae