May 02 2024

NETMANAGEIT

Intelligence Report

Eight Arms to Hold You: The Cuttlefish Malware

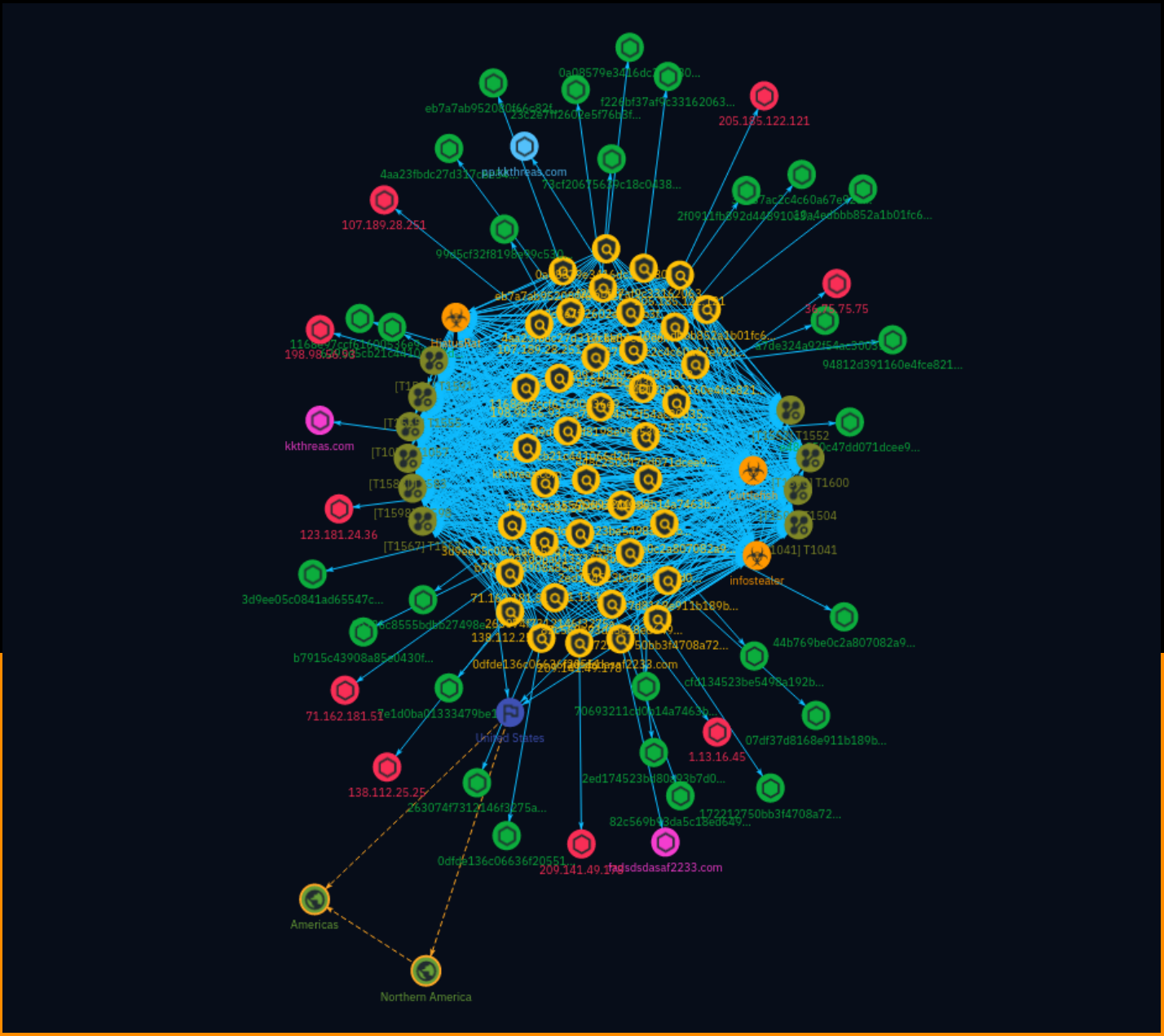

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The Black Lotus Labs team at Lumen Technologies is tracking a malware platform named Cuttlefish, targeting enterprise-grade small office/home office (SOHO) routers. This modular malware primarily steals authentication material from web requests transiting the router. It can also perform DNS and HTTP hijacking for connections to private IP spaces on internal networks. Cuttlefish overlaps with a previously reported activity cluster called HiatusRat, potentially linked to the interests of the People's Republic of China. While there is code overlap, shared victimology has not been observed between these two malware families.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

36.75.75.75

Description

- **Zip Code:** N/A - **ISP:** PT Telkom Indonesia - **ASN:** 7713 - **Organization:** PT Telkom Indonesia - **Is Crawler:** False - **Timezone:** Asia/Makassar - **Mobile:** False - **Host:** 36.75.75.75 - **Proxy:** False - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** ID - **Region:** North Kalimantan - **City:** Tarakan - **Latitude:** 3.3 - **Longitude:** 117.63

Pattern Type

stix

Pattern

[ipv4-addr:value = '36.75.75.75']

Name

138.112.25.25

Description

- **Zip Code:** N/A - **ISP:** FiberLink Ltd. - **ASN:** 198578 - **Organization:** FiberLink Ltd. - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** 138.112.25.25 - **Proxy:** True - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** District of Columbia - **City:** Washington - **Latitude:** 38.9 - **Longitude:** -77.04

Pattern Type

stix

Pattern

[ipv4-addr:value = '138.112.25.25']

Name

eb7a7ab952080f66c82fe8350da131ce0d7766f203bd4d97b0798b4f59283a27

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'eb7a7ab952080f66c82fe8350da131ce0d7766f203bd4d97b0798b4f59283a27']

Name

123.181.24.36

Description

- **Zip Code:** N/A - **ISP:** China Telecom - **ASN:** 4134 - **Organization:** China Telecom - **Is Crawler:** False - **Timezone:** Asia/Shanghai - **Mobile:** False -

Host: 123.181.24.36 - **Proxy:** False - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** CN - **Region:** Guangdong - **City:** Guangzhou - **Latitude:** 23.12 - **Longitude:** 113.25

Pattern Type

stix

Pattern

[ipv4-addr:value = '123.181.24.36']

Name

e48c250c47dd071dcee984a8e9f27b170004ff81c3f0da6a50364fdecf800fd3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e48c250c47dd071dcee984a8e9f27b170004ff81c3f0da6a50364fdecf800fd3']

Name

cfd134523be5498a192b212202746300d68da44965f465225b7e6a2fe1d9d296

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cfd134523be5498a192b212202746300d68da44965f465225b7e6a2fe1d9d296']

Name

b7915c43908a85e0430fa98cb0a08b24cfd3812662be1affa4ed9e135a31fb1e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b7915c43908a85e0430fa98cb0a08b24cfd3812662be1affa4ed9e135a31fb1e']

Name

a7de324a92f54ac30035e27a80a97329d30e21315f948cea636298b011998e90

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a7de324a92f54ac30035e27a80a97329d30e21315f948cea636298b011998e90']

Name

9b736c8555bdbb27498edcf5b074ed33b792e99436a2bb5691beb96d1d141365

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9b736c8555bdbb27498edcf5b074ed33b792e99436a2bb5691beb96d1d141365']

Name

99d5cf32f8198e99c530be4f5e05487e280bacdb8ef26aaf38dc20e301aad75f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '99d5cf32f8198e99c530be4f5e05487e280bacdb8ef26aaf38dc20e301aad75f']

Name

94812d391160e4fce821701b944cfd8f5fd9454b3cbb8e8974d1dc259310e500

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '94812d391160e4fce821701b944cfd8f5fd9454b3cbb8e8974d1dc259310e500']

Name

7e1d0ba01333479be1ddeb56de94e15204776245431480f59cd98f45ba956530

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7e1d0ba01333479be1ddeb56de94e15204776245431480f59cd98f45ba956530']

Name

73cf20675639c18c04381b5efd7d628736d149734280988f55358e301c1d9bb8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '73cf20675639c18c04381b5efd7d628736d149734280988f55358e301c1d9bb8']

Name

70693211cd0b14a7463b39b2fa801ce1fdefc85c7f3e003772d1b4deeb78efde

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '70693211cd0b14a7463b39b2fa801ce1fdefc85c7f3e003772d1b4deeb78efde']

Name

6295d5cb21c441066d2da81a76440bcac9bd5a7830fc9faea9668bd0b2015046

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6295d5cb21c441066d2da81a76440bcac9bd5a7830fc9faea9668bd0b2015046']

Name

4aa23fbdc27d317c6e54481b6d884b962adf6e691a4731c859ddaf9af09822c6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4aa23fbdc27d317c6e54481b6d884b962adf6e691a4731c859ddaf9af09822c6']

Name

44b769be0c2a807082a9bfd2f33fdc744552c5c7ca88a812ef4bd0393a50f132

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '44b769be0c2a807082a9bfd2f33fdc744552c5c7ca88a812ef4bd0393a50f132']

Name

3d9ee05c0841ad65547c0cc8516d092cff48dad5e7bbf97c99ddd44ee94a24bc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3d9ee05c0841ad65547c0cc8516d092cff48dad5e7bbf97c99ddd44ee94a24bc']

Name

37537ac2c4c60a67e92d5badae04f7f9115e97a67199b6f2c0010620c3eb0594

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '37537ac2c4c60a67e92d5badae04f7f9115e97a67199b6f2c0010620c3eb0594']

Name

1.13.16.45

Description

ISP: Shenzhen Tencent Computer Systems Company Limited **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLf8iODYvUpsTMZW230bPLg9 nll/NO0eEolK0U0M1j+KhW/acxXGXG6d32xPFYhxJogAncnYbl1zmQj/TIKLpvg= Fingerprint: 20:e9:b9:78:52:e6:de:85:fd:ab:6e:7c:33:d3:f6:f7 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 = '1.13.16.45']

Name

2f0911fb892d448910c36a37c9fbdec8c73ccfecc274854b1fa053fb1cc2369b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2f0911fb892d448910c36a37c9fbdec8c73ccfecc274854b1fa053fb1cc2369b']

Name

2ed174523bd80a93b7d09940d375f9c0d71e1ce8ecffb2320e02a78f4b601408

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2ed174523bd80a93b7d09940d375f9c0d71e1ce8ecffb2320e02a78f4b601408']

Name

263074f7312146f3275af64adbc5d02a618ed193ac84951c529ce8c367fb76e6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '263074f7312146f3275af64adbc5d02a618ed193ac84951c529ce8c367fb76e6']

Name

23c2e7ff2602e5f76b3f2c354761ef39966facb3b12ed05551816f482d4d5608

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '23c2e7ff2602e5f76b3f2c354761ef39966facb3b12ed05551816f482d4d5608']

Name

172212750bb3f4708a728d1d48ade3d6dd503d2892d4cc72d1719c06d5a1f4a8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '172212750bb3f4708a728d1d48ade3d6dd503d2892d4cc72d1719c06d5a1f4a8']

Name

1168e97ccf61600536e93e9c371ee7671bae4198d4bf566550328b241ec52e89

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1168e97ccf61600536e93e9c371ee7671bae4198d4bf566550328b241ec52e89']

Name

10a4edbbb852a1b01fc6fbf0aa1407bc8589432bddb2001ae62702f18d919e89

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '10a4edbbb852a1b01fc6fbf0aa1407bc8589432bddb2001ae62702f18d919e89']

Name

0dfde136c06636f2055153af4ad5f9bc2ed0ed2c055dde1fdbe82f866d0ebbac

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0dfde136c06636f2055153af4ad5f9bc2ed0ed2c055dde1fdbe82f866d0ebbac']

Name

0a08579e3416dc3cdd80c215b8fb94d86a0bb42c8c733530850417cffd6bde38

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0a08579e3416dc3cdd80c215b8fb94d86a0bb42c8c733530850417cffd6bde38']

Name

07df37d8168e911b189bbe0912b4842fa1fe48d5264e99738ad3247f9c818478

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '07df37d8168e911b189bbe0912b4842fa1fe48d5264e99738ad3247f9c818478']

Name

kkthreas.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': '4 months ago', 'timestamp': 1703054762, 'iso': '2023-12-20T01:46:02-05:00'} - **IPQS: Domain:** kkthreas.com - **IPQS: IP Address:** 198.98.56.93

Pattern Type

stix

Pattern

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

Name

pp.kkthreas.com

Pattern Type

stix

Pattern

[hostname:value = 'pp.kkthreas.com']

Name

fadsdsdasaf2233.com

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': '3 hours ago', 'timestamp': 1714646748, 'iso': '2024-05-02T06:45:48-04:00'} - **IPQS: Domain:** fadsdsdasaf2233.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'fadsdsdasaf2233.com']

Name

209.141.49.178

Description

ISP: FranTech Solutions **OS:** - ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDygy8iG9NU04HZqBcmfe3cGt/q8qTnObuAnk5l1dvZoTjJXzyelHaSIazG+IVbeQP9sZ69qWKudzQK33x4276l8b6eXpRfFpKth/RPRvKg41rMf0nCx3fpYQPG7nQ5Z5ifi4Qg9sBEbqMjtZ7UKnUfNDIL35XdMuzvWLdNGZLlprGsrVVfWYjqE+D269KWS8fI6VazBFdgf3Zad592YXJAhf/9ZXhC3FKsTiY0LZCYW4+gkTwHU/iGww5TPE7oLGp4jqGcUmN76ubOlodftE7tt8+cNnmMu7ImVlc0yBBl2qnyhXKcEnoWuUx9/kQMsx+F0Ga+kxIJ6S8MCbjsxmhui0TUMCpQVMnKzG37Gqm1BX8Zrj9lu50xtY4NMR9cuJVrGqQoWZ5n7IYNllsFHQjrR+RPaEatMBfKBaMDCnQFkS8npkc0zvZ7Svla8pqLHnf6HXxhh2qxdCGQIxnIzTC+AXFqf8xJDICf8XY1my5iglAxoQJ8jlQ21GY5iSoz08s= Fingerprint: f3:1d:d6:27:6b:34:9f:c2:90:be:fb:90:c7:62:29:19 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/1.1 404 Not Found Content-Type: text/plain; charset=utf-8 X-Content-Type-Options: nosniff Date: Thu, 18 Apr 2024 15:09:49 GMT Content-Length: 15 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '209.141.49.178']

Name

205.185.122.121

Description

- **Zip Code:** N/A - **ISP:** FranTech Solutions - **ASN:** 53667 - **Organization:** FranTech Solutions - **Is Crawler:** False - **Timezone:** America/Los_Angeles - **Mobile:** False - **Host:** 205.185.122.121 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Nevada - **City:** Las Vegas - **Latitude:** 35.93 - **Longitude:** -114.97

Pattern Type

stix

Pattern

[ipv4-addr:value = '205.185.122.121']

Name

198.98.56.93

Description

ISP: FranTech Solutions **OS:** Ubuntu ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDx8cvGMu2fMJ4cCz+LxB+DoDKZwuhdbngWZ3K+n6lgR MLS BTG5bexEoU/FqaE8IzuFWQ1A+3vZZelBCglShAdjlUQLowFtsn2D3aeg75VsyT6Arl7uq69JRiL7 VlsS0iuhIvE8z5UKyPMXUIS3dq9qgLo7MrHvcvmmvSFXURVEBOJKeUTp2iUw/Zopgrw8Ey/BpJ4p Q/cVwWbrx+Bld0u+63euqef1WAihzkQUVn7R6s25t2Ce0ZGfnxu0vKmBKE2zlZ+/wuR+G6fX9M5t 2gNGT+2h5LAOEQUaHH7jnqJn6iIQfJR1JXAq3DF/LnlpDTlito2jeP6mqqzk9g28sk8aKSdKpPQ+ LAzz3/WRUTVmwzCYAwKejdjrMw56wIhTzgzne832gC7hV7HdpNp2EaMs4zZEyIoo7JClEWPQN4p3 3uqzGp9Cp45OOCIgUQ1HRbchMjUE0Gz1bzVBYOPcpUbwgsz8nv2K7LmUu3RTpAp833M1PYvjqN 3G JU5onilS4Y0= Fingerprint: 3b:9b:e7:84:15:3b:49:f6:50:d1:73:37:8a:a7:a5:e7 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 ``` ---------- **443:** ``` HTTP/1.1 400 Bad Request Server: nginx/1.18.0 (Ubuntu) Date: Tue, 23 Apr 2024 13:55:26 GMT Content-Type: text/html Content-Length: 648 Connection: close ``` HEARTBLEED: 2024/04/23 13:55:34 198.98.56.93:443 - SAFE ---------- **8000:** ``` HTTP/1.1 405 Method Not Allowed date: Sun, 14 Apr 2024 00:46:58 GMT server: uvicorn allow: POST content-length: 31 content-type: application/json ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '198.98.56.93']

Name

107.189.28.251

Description

- **Zip Code:** N/A - **ISP:** FranTech Solutions - **ASN:** 53667 - **Organization:** FranTech Solutions - **Is Crawler:** False - **Timezone:** Europe/Luxembourg - **Mobile:** False - **Host:** 107.189.28.251 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** True - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** LU - **Region:** Luxembourg - **City:** Luxembourg - **Latitude:** 49.61 - **Longitude:** 6.13

Pattern Type

stix

Pattern

[ipv4-addr:value = '107.189.28.251']

Name

71.162.181.51

Description

- **Zip Code:** N/A - **ISP:** Verizon Fios Business - **ASN:** 701 - **Organization:** Verizon Fios Business - **Is Crawler:** False - **Timezone:** America/New_York - **Mobile:** False - **Host:** static-71-162-181-51.phlapa.fios.verizon.net - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** Pennsylvania - **City:** Brookhaven - **Latitude:** 39.86669922 - **Longitude:** -75.38619995

Pattern Type

stix

Pattern

[ipv4-addr:value = '71.162.181.51']

Name

f226bf37af9c33162063db3eb018fed7f088f86d0a20ca54c013fda96c7f2e05

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f226bf37af9c33162063db3eb018fed7f088f86d0a20ca54c013fda96c7f2e05']

Name
82c569b93da5c18ed649ebd4c2c79437db4611a6a1373e805a3cb001c64130b7
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '82c569b93da5c18ed649ebd4c2c79437db4611a6a1373e805a3cb001c64130b7']

Attack-Pattern

Name
T1504
ID
T1504
Name
T1598
ID
T1598
Description
Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from [Phishing](https://attack.mitre.org/techniques/T1566) in that the objective is gathering data from the victim rather than executing malicious code. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass credential harvesting campaigns. Adversaries may also try to obtain information directly through the exchange of emails, instant messages, or other electronic conversation means.(Citation: ThreatPost Social Media Phishing)(Citation:

TrendMictro Phishing)(Citation: PCMag FakeLogin)(Citation: Sophos Attachment)(Citation: GitHub Phishery) Victims may also receive phishing messages that direct them to call a phone number where the adversary attempts to collect confidential information.(Citation: Avertium callback phishing) Phishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) and/or sending multiple, seemingly urgent messages. Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Phishing for information may also involve evasive techniques, such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)). (Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014)

Name

T1591

ID

T1591

Description

Adversaries may gather information about the victim's organization that can be used during targeting. Information about an organization may include a variety of details, including the names of divisions/departments, specifics of business operations, as well as the roles and responsibilities of key employees. Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about an organization may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: ThreatPost Broadvoice Leak)(Citation: SEC EDGAR Search) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593)), establishing operational resources (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)),

and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566) or [Trusted Relationship](https://attack.mitre.org/techniques/T1199)).

Name

T1041

ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

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. Administrator or otherwise elevated access may provide better process details. 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

T1552

ID

T1552

Description

Adversaries may search compromised systems to find and obtain insecurely stored credentials. These credentials can be stored and/or misplaced in many locations on a system, including plaintext files (e.g. [Bash History](https://attack.mitre.org/techniques/T1552/003)), operating system or application-specific repositories (e.g. [Credentials in Registry](https://attack.mitre.org/techniques/T1552/002)), or other specialized files/artifacts (e.g. [Private Keys](https://attack.mitre.org/techniques/T1552/004)).(Citation: Brining MimiKatz to Unix)

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

T1555

ID

T1555

Description

Adversaries may search for common password storage locations to obtain user credentials.(Citation: F-Secure The Dukes) Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications and services that store passwords to make them easier for users to manage and maintain, such as password managers and cloud secrets vaults. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

Name

T1600

ID

T1600

Description

Adversaries may compromise a network device's encryption capability in order to bypass encryption that would otherwise protect data communications. (Citation: Cisco Synful Knock Evolution) Encryption can be used to protect transmitted network traffic to maintain its confidentiality (protect against unauthorized disclosure) and integrity (protect against unauthorized changes). Encryption ciphers are used to convert a plaintext message to ciphertext and can be computationally intensive to decipher without the associated

decryption key. Typically, longer keys increase the cost of cryptanalysis, or decryption without the key. Adversaries can compromise and manipulate devices that perform encryption of network traffic. For example, through behaviors such as [Modify System Image](https://attack.mitre.org/techniques/T1601), [Reduce Key Space](https://attack.mitre.org/techniques/T1600/001), and [Disable Crypto Hardware](https://attack.mitre.org/techniques/T1600/002), an adversary can negatively effect and/or eliminate a device's ability to securely encrypt network traffic. This poses a greater risk of unauthorized disclosure and may help facilitate data manipulation, Credential Access, or Collection efforts. (Citation: Cisco Blog Legacy Device Attacks)

Name

T1583

ID

T1583

Description

Adversaries may buy, lease, rent, or obtain infrastructure that can be used during targeting. A wide variety of infrastructure exists for hosting and orchestrating adversary operations. Infrastructure solutions include physical or cloud servers, domains, and third-party web services.(Citation: TrendmicroHideoutsLease) Some infrastructure providers offer free trial periods, enabling infrastructure acquisition at limited to no cost.(Citation: Free Trial PurpleUrchin) Additionally, botnets are available for rent or purchase. Use of these infrastructure solutions allows adversaries to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal, such as contacting third-party web services or acquiring infrastructure to support [Proxy](https://attack.mitre.org/techniques/T1090), including from residential proxy services. (Citation: amnesty_nso_pegasus)(Citation: FBI Proxies Credential Stuffing)(Citation: Mandiant APT29 Microsoft 365 2022) Depending on the implementation, adversaries may use infrastructure that makes it difficult to physically tie back to them as well as utilize infrastructure that can be rapidly provisioned, modified, and shut down.

Malware

Name
Cuttlefish

Name
HiatusRat

Name
infostealer

Country

Name
United States

Region

Name
Northern America

Name
Americas

IPv4-Addr

Value
36.75.75.75
138.112.25.25
123.181.24.36
1.13.16.45
209.141.49.178
205.185.122.121
198.98.56.93
107.189.28.251
71.162.181.51

StixFile

Value
eb7a7ab952080f66c82fe8350da131ce0d7766f203bd4d97b0798b4f59283a27
e48c250c47dd071dcee984a8e9f27b170004ff81c3f0da6a50364fdecf800fd3
cfd134523be5498a192b212202746300d68da44965f465225b7e6a2fe1d9d296
b7915c43908a85e0430fa98cb0a08b24cfd3812662be1affa4ed9e135a31fb1e
a7de324a92f54ac30035e27a80a97329d30e21315f948cea636298b011998e90
9b736c8555bdbb27498edcf5b074ed33b792e99436a2bb5691beb96d1d141365
99d5cf32f8198e99c530be4f5e05487e280bacdb8ef26aaf38dc20e301aad75f
94812d391160e4fce821701b944cfd8f5fd9454b3cbb8e8974d1dc259310e500
7e1d0ba01333479be1ddeb56de94e15204776245431480f59cd98f45ba956530
73cf20675639c18c04381b5efd7d628736d149734280988f55358e301c1d9bb8
70693211cd0b14a7463b39b2fa801ce1fdefc85c7f3e003772d1b4deeb78efde
6295d5cb21c441066d2da81a76440bcac9bd5a7830fc9faea9668bd0b2015046
4aa23fbdc27d317c6e54481b6d884b962adf6e691a4731c859ddaf9af09822c6

44b769be0c2a807082a9bfd2f33fdc744552c5c7ca88a812ef4bd0393a50f132

3d9ee05c0841ad65547c0cc8516d092cff48dad5e7bbf97c99ddd44ee94a24bc

37537ac2c4c60a67e92d5badae04f7f9115e97a67199b6f2c0010620c3eb0594

2f0911fb892d448910c36a37c9fbdec8c73ccfecc274854b1fa053fb1cc2369b

2ed174523bd80a93b7d09940d375f9c0d71e1ce8ecffb2320e02a78f4b601408

263074f7312146f3275af64adbc5d02a618ed193ac84951c529ce8c367fb76e6

23c2e7ff2602e5f76b3f2c354761ef39966facb3b12ed05551816f482d4d5608

172212750bb3f4708a728d1d48ade3d6dd503d2892d4cc72d1719c06d5a1f4a8

1168e97ccf61600536e93e9c371ee7671bae4198d4bf566550328b241ec52e89

10a4edbbb852a1b01fc6fbf0aa1407bc8589432bddb2001ae62702f18d919e89

0dfde136c06636f2055153af4ad5f9bc2ed0ed2c055dde1fdbe82f866d0ebbac

0a08579e3416dc3cdd80c215b8fb94d86a0bb42c8c733530850417cffd6bde38

07df37d8168e911b189bbe0912b4842fa1fe48d5264e99738ad3247f9c818478

f226bf37af9c33162063db3eb018fed7f088f86d0a20ca54c013fda96c7f2e05

82c569b93da5c18ed649ebd4c2c79437db4611a6a1373e805a3cb001c64130b7

Hostname

Value
pp.kkthreas.com

Domain-Name

Value
kkthreas.com
fadsdsdasaf2233.com

External References

- https://github.com/blacklotuslabs/IOCs/blob/main/Cuttlefish_IOCs.txt
- https://blog.lumen.com/eight-arms-to-hold-you-the-cuttlefish-malware/
- https://otx.alienvault.com/pulse/66339a3fb48f836792b3116a