Sep 01 2023

NETMANAGEIT

Intelligence Report

An Ongoing Open Source Attack Reveals Roots Dating Back To 2021

Table of contents

Overview

- Description 4
- Confidence 4

Entities

- Indicator 5
- Attack-Pattern 16

Observables

- Domain-Name 20
- Hostname 21
- IPv4-Addr 22

External References

- External References 23

Overview

Description

In an ongoing campaign, a threat actor is leveraging npm packages to target developers to steal source code and secrets.

Confidence

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

15 / 100

Indicator

Name

cczk46g2vtc0000k68dgggx31deyyyyyb.oast.fun

Pattern Type

stix

Pattern

[hostname:value = 'cczk46g2vtc0000k68dgggx31deyyyyyb.oast.fun']

Name

65.21.108.160

Description

ISP: Hetzner Online GmbH **OS:** None ---------- Hostnames: - static.160.108.21.65.clients.your-server.de ---------- Domains: - your-server.de ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCx9PPuVl/MpxFpwWxLmqB5Ram79xY5RjN79aGozJMWu8fg vZpzicj9RY+MHbBRYITsLLKAJ7vV2bDtjDiiVvf5vefw1mxp2Pk/SAwCS+LN4skvF5r+mX6X7TOA w8OC5t+Ewvjmwd0r2nGwIrB/Zdzb99AUd6F4D9BosHwOfa1gVprtB3lkP5z/tghmHZg2cN46z1mG 5z7lbtI2C512cehYA4lL9MN0qN9YPKoXDsjMIRzAHl9H2fTYXvjzi+8c9xkcSgxGLMsMiK4g8+EY 6GmEzjAP+5vJhCk5fmO/9dhCkbUNqDZfX1iyQAkc4ulFkv+gKLxaBXOX1WQH/RRzRX3t Fingerprint: c0:95:05:a2:74:a1:63:7a:a3:4b:31:f0:94:f3:ba:f2 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521

diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Sun, 27 Aug 2023 01:53:25 GMT Content-Type: text/html Content-Length: 5658 Last-Modified: Tue, 06 Dec 2022 12:31:52 GMT Connection: keep-alive ETag: "638f3638-161a" Accept-Ranges: bytes ``` ----------

Pattern Type
stix

Pattern
[ipv4-addr:value = '65.21.108.160']

Name
efrva6.dnslog.cn

Pattern Type
stix

Pattern
[hostname:value = 'efrva6.dnslog.cn']

Name
5.9.104.19

Description

ISP: Hetzner Online GmbH **OS:** None ---------- Hostnames: - static.19.104.9.5.clients.your-server.de ---------- Domains: - your-server.de ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Mon, 21 Aug 2023 11:52:35 GMT Content-Type: text/html Content-Length: 612 Last-Modified: Mon, 13 Sep 2021 23:10:10 GMT Connection: keep-alive ETag: "613fda52-264" X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Accept-Ranges: bytes ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.9.104.19']

Name

c7kxnys58daceezcxx0jjstn6ec50vok.oastify.com

Pattern Type

stix

Pattern

[hostname:value = 'c7kxnys58daceezcxx0jjstn6ec50vok.oastify.com']

Name

6wxd3v84nevku06dcgbqcxrmt.canarytokens.com

Pattern Type

stix

Pattern

[hostname:value = '6wxd3v84nevku06dcgbqcxrmt.canarytokens.com']

Name

288utkkrohmp0nr8znflcp88nztrhg.oastify.com

Pattern Type

stix

Pattern

[hostname:value = '288utkkrohmp0nr8znflcp88nztrhg.oastify.com']

Name

cup1qnm56sdo4bdv.b.requestbin.net

Pattern Type

stix

Pattern

[hostname:value = 'cup1qnm56sdo4bdv.b.requestbin.net']

Name

198.199.83.132

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_9.0p1 Ubuntu-1ubuntu7.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNw7OaGeoyL8op1LBuO1+Ris x942tvZNxaptxT2AMnWL1ro++CNo8vRNK5cbUPKZJTbWdq74kVazg1Z5Cn2Pu70= Fingerprint: 0d:49:a2:08:15:c8:51:c2:46:62:fd:a9:51:8b:9c:9d Kex Algorithms: sntrup761x25519-sha512@openssh.com 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 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 ``` ---------- **53:** ``` 9.18.4-2ubuntu2.1-Ubuntu Recursion: enabled Resolver name: subdomains ``` ---------- **53:** ``` 9.18.12-0ubuntu0.22.10.2-Ubuntu Recursion: enabled Resolver name: subdomains ``` ---------- **80:** ``` HTTP/1.1 301 Moved Permanently Location: https://198.199.83.132/ Content-Type: text/html; charset=utf-8 Date: Tue, 29 Aug 2023 19:50:41 GMT Connection: keep-alive Keep-Alive: timeout=5 Content-Length: 221 ``` ---------- **443:** ``` ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '198.199.83.132']

Name

4or5o5yn5lqzenk4.b.requestbin.net

Pattern Type

stix

Pattern

[hostname:value = '4or5o5yn5lqzenk4.b.requestbin.net']

Name

185.62.56.25

Description

ISP: Snel.com B.V. **OS:** None ------------------------- Hostnames: - host.pornohd.com ------------------------- Domains: - pornohd.com ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.3 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBMKQUrnpZ8kJfPYCexWEYP7u oXL7hklis7wZFjt9pN1wMMNXneDG5d78PFFnYNPsdj9yTEnCnMG90+5ZIGVPwSw= Fingerprint: 67:bc:e1:56:92:f6:9a:ee:20:23:2b:05:2f:1f:f7:52 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ------------------ **5000:** ``` HTTP/1.1 403 FORBIDDEN Server: Werkzeug/2.3.6 Python/3.10.12 Date: Sat, 26 Aug 2023 01:57:31 GMT Content-Type: text/html; charset=utf-8 Content-Length: 213 Connection: close ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.62.56.25']

Name

bind9-or-callback-server.com

Pattern Type

stix

Pattern

[domain-name:value = 'bind9-or-callback-server.com']

Name

bq5m9lnmalh9ktyi9wydockt9kfb32rr.oastify.com

Pattern Type

stix

Pattern

[hostname:value = 'bq5m9lnmalh9ktyi9wydockt9kfb32rr.oastify.com']

Name

ck0r1hp2vtc00007c0zggjocy3ryyyyyb.oast.fun

Pattern Type

stix

Pattern

[hostname:value = 'ck0r1hp2vtc00007c0zggjocy3ryyyyyb.oast.fun']

Name

178.128.27.205

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDkOkA5bHPtYcplw6F4qwpiaItHkyfLu+l6ciQCbeuEAJyRyQppGkaeSBMi88jn3DEoLzsF8kHETmgpXNm/aDXnD94MXfdHCNtk+Kn3R9Fr5Bljki09EVkZTNGsDC1rvZ05V0MAwyUWynXnrWX6T7KlZlvyNT5MTlVPhFhx8Sbneqdh0TxTwzCFHw95EpcNo7e+gBMQ vPkc/ E3vDOnXam9Y2zU04Nq2KF+9JD6MNGr+qkIWVM0GjLwAjADHjEL5rZj5Etoym94qTqdb7m+FLdzF3R4Z83nvFUEIwxT3zE/yHkxlQ+aYs55w2IOLeC3e4M8U3JvjLJ9dWPfyly24T6/7 Fingerprint: 01:7b:b8:0c:e1:cc:53:50:72:0c:88:8b:60:94:7f:0a Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **111:** ``` Portmap Program Version Protocol Port portmapper 4 tcp 111 portmapper 3 tcp 111 portmapper 2 tcp 111 portmapper 4 udp 111 portmapper 3 udp 111 portmapper 2 udp 111 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '178.128.27.205']

Name

1wy3rk316x8qqy4fyxtvcs4kkbq2es2h.oastify.com

Pattern Type

stix

Pattern

[hostname:value = '1wy3rk316x8qqy4fyxtvcs4kkbq2es2h.oastify.com']

Name

51.250.2.204

Description

ISP: Yandex.Cloud LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 200 OK Server: nginx/1.18.0 (Ubuntu) Date: Mon, 14 Aug 2023 19:30:56 GMT Content-Type: text/html Content-Length: 612 Last-Modified: Fri, 02 Jun 2023 10:34:57 GMT Connection: keep-alive ETag: "6479c5d1-264" Accept-Ranges: bytes ``` ---------- **2020:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.3 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBP4LyQ7KduBo+EmDFfNC5k/L M3lanV5AGtXFJ3A983dgEmezIXZTAaKu3mpqLq0SMSGzn+tNB3+uBwwb0g9Pe0o= Fingerprint: 8a:8f:69:c3:0a:e8:ba:89:19:76:a6:c3:e8:04:b8:73 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **8888:** ``` HTTP/1.1 200 OK Date: Thu, 03 Aug 2023 13:40:56 GMT Content-Length: 0 ``` ---------- **30002:** ``` HTTP/1.1 404 Not Found date: Thu, 10 Aug 2023 08:05:41 GMT server: uvicorn content-length: 22 content-type: application/json ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '51.250.2.204']

Name

185.62.57.60

Description

ISP: Snel.com B.V. **OS:** None ------------------------- Hostnames: - test-backup.mila362.com ------------------------- Domains: - mila362.com ------------------------- Services: **21:** ``` 220 pyftpdlib 1.5.7 ready. 530 Anonymous access not allowed. 214-The following commands are recognized: ABOR ALLO APPE CDUP CWD DELE EPRT EPSV FEAT HELP LIST MDTM MFMT MKD MLSD MLST MODE NLST NOOP OPTS PASS PASV PORT PWD QUIT REIN REST RETR RMD RNFR RNTO SITE SIZE STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD XPWD XRMD 214 Help command successful. 211-Features supported: EPRT EPSV MDTM MFMT MLST type*;perm*;size*;modify*;unique*;unix.mode;unix.uid;unix.gid; REST STREAM SIZE TVFS UTF8 211 End FEAT. ``` ------------------ **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.3 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBtpjr92PuSP2VyiIZF2slMk OyxWZMlh6uwOpnKydCO159UagXI3lmKZkoJHiQB/tPcF52EwnOXK5MtzOUUJN4A= Fingerprint: f1:4d:fd:00:c1:9b:c3:3a:7e:6a:85:4d:82:6d:75:8f Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ------------------ **8000:** ``` HTTP/1.1 404 NOT

FOUND Server: Werkzeug/2.3.6 Python/3.10.12 Date: Sun, 13 Aug 2023 22:11:17 GMT Content-Type: text/html; charset=utf-8 Content-Length: 207 Connection: close ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.62.57.60']

Name

fhg62xavat9jzyt6euwxi6sro.canarytokens.com

Pattern Type

stix

Pattern

[hostname:value = 'fhg62xavat9jzyt6euwxi6sro.canarytokens.com']

Attack-Pattern

Name
Audio Capture
ID
T1123
Description
An adversary can leverage a computer's peripheral devices (e.g., microphones and webcams) or applications (e.g., voice and video call services) to capture audio recordings for the purpose of listening into sensitive conversations to gather information. Malware or scripts may be used to interact with the devices through an available API provided by the operating system or an application to capture audio. Audio files may be written to disk and exfiltrated later.
Name
Input Capture
ID
T1056
Description
Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various

different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

Name

Masquerading

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)

Name

Indicator Removal

ID

T1070

Description

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from

downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. 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 malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as 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) 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) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Resource Hijacking

ID

T1496

Description

Adversaries may leverage the resources of co-opted systems in order to solve resource intensive problems, which may impact system and/or hosted service availability. One common purpose for Resource Hijacking is to validate transactions of cryptocurrency networks and earn virtual currency. Adversaries may consume enough system resources to negatively impact and/or cause affected machines to become unresponsive.(Citation: Kaspersky Lazarus Under The Hood Blog 2017) Servers and cloud-based systems are common targets because of the high potential for available resources, but user endpoint systems may also be compromised and used for Resource Hijacking and cryptocurrency mining.(Citation: CloudSploit - Unused AWS Regions) Containerized environments may also be targeted due to the ease of deployment via exposed APIs and the potential for scaling mining activities by deploying or compromising multiple containers within an environment or cluster.(Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro Exposed Docker APIs) Additionally, some cryptocurrency mining malware identify then kill off processes for competing malware to ensure it’s not competing for resources.(Citation: Trend Micro War of Crypto Miners) Adversaries may also use malware that leverages a system's network bandwidth as part of a botnet in order to facilitate [Network Denial of Service](https://attack.mitre.org/techniques/T1498) campaigns and/or to seed malicious torrents.(Citation: GoBotKR)

Domain-Name

Value
bind9-or-callback-server.com

Hostname

Value
cczk46g2vtc0000k68dgggx31deyyyyyb.oast.fun
4or5o5yn5lqzenk4.b.requestbin.net
ck0r1hp2vtc00007c0zggjocy3ryyyyyb.oast.fun
bq5m9lnmalh9ktyi9wydockt9kfb32rr.oastify.com
c7kxnys58daceezcxx0jjstn6ec50vok.oastify.com
fhg62xavat9jzyt6euwxi6sro.canarytokens.com
efrva6.dnslog.cn
288utkkrohmp0nr8znflcp88nztrhg.oastify.com
1wy3rk316x8qqy4fyxtvcs4kkbq2es2h.oastify.com
cup1qnm56sdo4bdv.b.requestbin.net
6wxd3v84nevku06dcgbqcxrmt.canarytokens.com

IPv4-Addr

Value
51.250.2.204
5.9.104.19
185.62.57.60
198.199.83.132
185.62.56.25
65.21.108.160
178.128.27.205

External References

- https://otx.alienvault.com/pulse/64f09d12f52704036d29d312
- https://checkmarx.com/blog/an-ongoing-open-source-attack-reveals-roots-dating-back-to-2021/