Jul 03 2023

NETMANAGEIT

Intelligence Report

Meduza Stealer or The Return of The Infamous Aurora Stealer

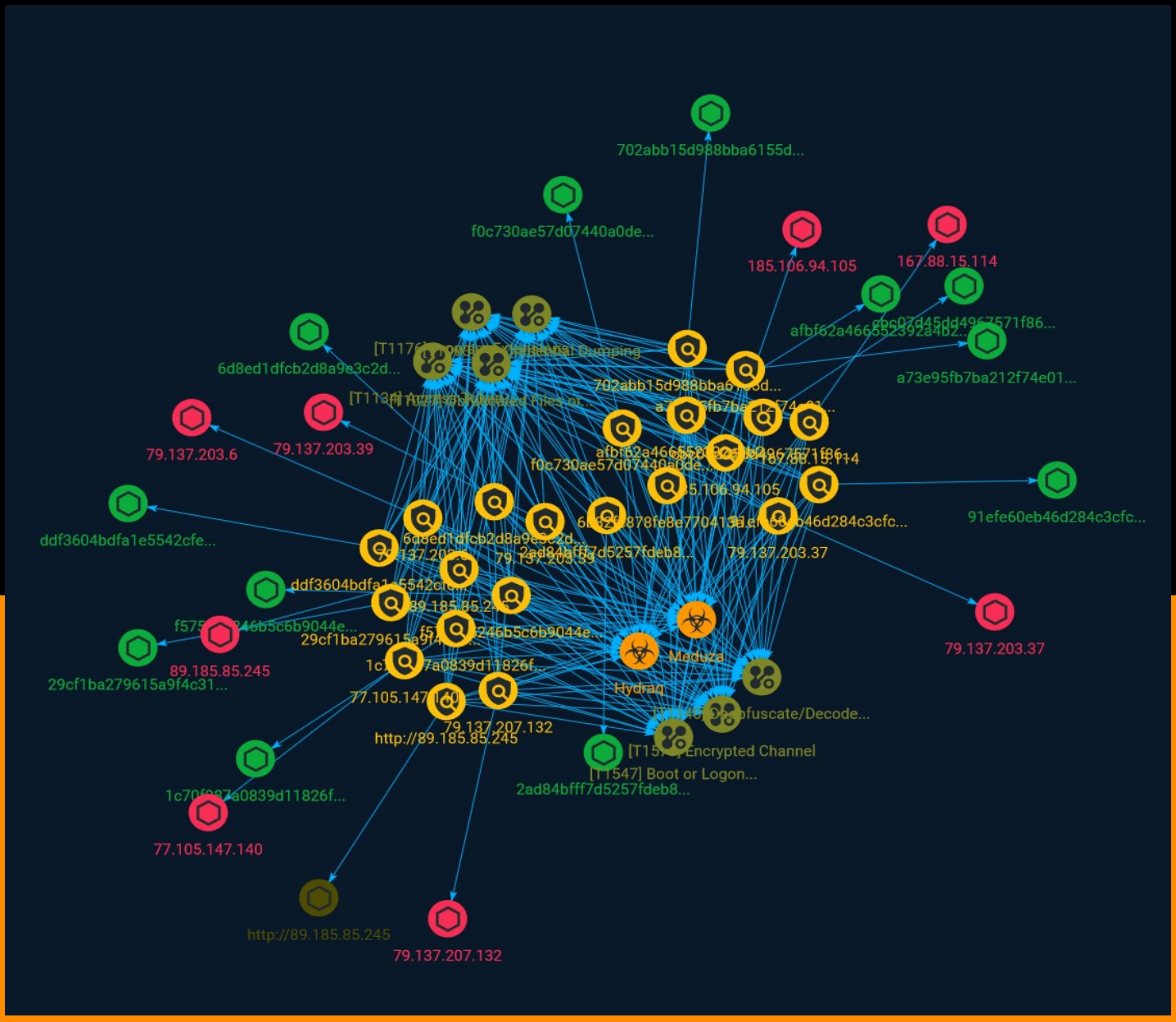

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A new stealer, which collects data from more than 100 cryptowallets, is being developed by the Russian-speaking community, as well as being designed to make it easier to detect.

Confidence

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

15 / 100

Indicator

Name

79.137.203.39

Description

ISP: AEZA GROUP Ltd **OS:** Windows (build 10.0.19041) ---------- Hostnames: - joyous-produce.aeza.network ---------- Domains: - aeza.network ---------- Services: **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10 (version 2004)/Windows Server (version 2004) OS Build: 10.0.19041 Target Name: WIN-X8HD67KBF7 NetBIOS Domain Name: WIN-X8HD67KBF7 NetBIOS Computer Name: WIN-X8HD67KBF7 DNS Domain Name: WIN-X8HD67KBF7 FQDN: WIN-X8HD67KBF7 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '79.137.203.39']

Name

f575eb5246b5c6b9044ea04610528c040c982904a5fb3dc1909ce2f0ec15c9ef

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f575eb5246b5c6b9044ea04610528c040c982904a5fb3dc1909ce2f0ec15c9ef']

Name

6d8ed1dfcb2d8a9e3c2d51fa106b70a685cbd85569ffabb5692100be75014803

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6d8ed1dfcb2d8a9e3c2d51fa106b70a685cbd85569ffabb5692100be75014803']

Name

2ad84bfff7d5257fdeb81b4b52b8e0115f26e8e0cdaa014f9e3084f518aa6149

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2ad84bfff7d5257fdeb81b4b52b8e0115f26e8e0cdaa014f9e3084f518aa6149']

Name

79.137.207.132

Description

CC=DE ASN=AS210644 AEZA GROUP Ltd

Pattern Type

stix

Pattern

[ipv4-addr:value = '79.137.207.132']

Name

f0c730ae57d07440a0de0889db93705c1724f8c3c628ee16a250240cc4f91858

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f0c730ae57d07440a0de0889db93705c1724f8c3c628ee16a250240cc4f91858']

Name

185.106.94.105

Description

ISP: AEZA GROUP Ltd **OS:** None ---------- Hostnames: - just-giraffe.aeza.network ---------- Domains: - aeza.network ---------- Services: **8429:** ``` HTTP/1.1 200 OK X-Server-Hostname: just-

giraffe.aeza.network Date: Sun, 02 Jul 2023 10:41:40 GMT Content-Length: 460 Content-Type: text/plain; charset=utf-8 ``` ---------- **9100:** ``` HTTP/1.1 400 Bad Request Content-Type: text/plain; charset=utf-8 Connection: close 400 Bad Request Prometheus Node Exporter: node_exporter_build_info: branch: HEAD goversion: go1.15.8 revision: b597c1244d7bef49e6f3359c87a56dd7707f6719 version: 1.1.2 node_uname_info: domainname: (none) machine: x86_64 nodename: just-giraffe.aeza.network release: 5.4.0-139-generic sysname: Linux version: #156-Ubuntu SMP Fri Jan 20 17:27:18 UTC 2023 node_network_info: lo: address: 00:00:00:00:00:00 broadcast: 00:00:00:00:00:00 device: lo operstate: unknown ens3: address: 52:54:00:17:28:8b broadcast: ff:ff:ff:ff:ff:ff device: ens3 duplex: unknown operstate: up ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.106.94.105']

Name

29cf1ba279615a9f4c31d6441dd7c93f5b8a7d95f735c0daa3cc4dbb799f66d4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '29cf1ba279615a9f4c31d6441dd7c93f5b8a7d95f735c0daa3cc4dbb799f66d4']

Name

cbc07d45dd4967571f86ae75b120b620b701da11c4ebfa9afcae3a0220527972

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cbc07d45dd4967571f86ae75b120b620b701da11c4ebfa9afcae3a0220527972']

Name

79.137.203.37

Description

ISP: AEZA GROUP Ltd **OS:** Windows (build 10.0.19041) ---------- Hostnames: - trite-powder.aeza.network ---------- Domains: - aeza.network ---------- Services: **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10 (version 2004)/Windows Server (version 2004) OS Build: 10.0.19041 Target Name: WIN-X8HD67KBF7 NetBIOS Domain Name: WIN-X8HD67KBF7 NetBIOS Computer Name: WIN-X8HD67KBF7 DNS Domain Name: WIN-X8HD67KBF7 FQDN: WIN-X8HD67KBF7 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '79.137.203.37']

Name

89.185.85.245

Description

ISP: AEZA GROUP Ltd **OS:** Windows (build 10.0.19041) ---------- Hostnames: - hurt-impulse.aeza.network ---------- Domains: - aeza.network ---------- Services: **80:** ``` HTTP/1.1 404 content-type: text/html; charset=utf-8 content-length: 207 date: Mon, 26 Jun 2023 02:31:47 GMT server: hypercorn-h11 ``` ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10 (version 2004)/Windows Server (version 2004) OS Build: 10.0.19041 Target Name: WINDOWS-C6OJF5R NetBIOS Domain Name: WINDOWS-C6OJF5R NetBIOS Computer Name: WINDOWS-C6OJF5R DNS Domain Name: WINDOWS-C6OJF5R FQDN: WINDOWS-C6OJF5R ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '89.185.85.245']

Name

91efe60eb46d284c3cfcb584d93bc5b105bf9b376bee761c504598d064b918d4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '91efe60eb46d284c3cfcb584d93bc5b105bf9b376bee761c504598d064b918d4']

Name

1c70f987a0839d11826f053ae90e81a277fa154f5358303fe9a511dbe8b529f2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1c70f987a0839d11826f053ae90e81a277fa154f5358303fe9a511dbe8b529f2']

Name

702abb15d988bba6155dd440f615bbfab9f3c0ed662fc3e64ab1289a1098af98

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '702abb15d988bba6155dd440f615bbfab9f3c0ed662fc3e64ab1289a1098af98']

Name

6b82fc878fe8e770413a716e2966d61e8a857950

Description

Detects MeduzaStealer

Pattern Type

yara

Pattern

rule MeduzaStealer { meta: author = "RussianPanda" description = "Detects MeduzaStealer" date = "6/27/2023" strings: $s1 = {74 69 6D 65 7A 6F 6E 65} $s2 = {75 73 65 72 5F 6E 61 6D 65} $s3 = {67 70 75} $s4 = {63 75 72 72 65 6E 74 5F 70 61 74 68 28 29} $s5 = {C5 FD EF} $s6 = {66 0F EF} condition: all of them and filesize < 700KB }

Name

ddf3604bdfa1e5542cfee4d06a4118214a23f1a65364f44e53e0b68cbfc588ea

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ddf3604bdfa1e5542cfee4d06a4118214a23f1a65364f44e53e0b68cbfc588ea']

Name

a73e95fb7ba212f74e0116551ccba73dd2ccba87d8927af29499bba9b3287ea7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a73e95fb7ba212f74e0116551ccba73dd2ccba87d8927af29499bba9b3287ea7']

Name

http://89.185.85.245

Pattern Type

stix

Pattern

[url:value = 'http://89.185.85.245']

Name

79.137.203.6

Description

ISP: AEZA GROUP Ltd **OS:** Windows (build 10.0.19041) ---------- Hostnames: - motionless-hand.aeza.network - rad-winter.aeza.network ---------- Domains: - aeza.network ---------- Services: **443:** ``` HTTP/1.1 400 Bad Request Content-Type: text/plain; charset=utf-8 Sec-Websocket-Version: 13 X-Content-Type-Options: nosniff Date: Thu, 22 Jun 2023 19:29:12 GMT Content-Length: 12 Bad Request ``` ---------- **2052:** ``` HTTP/1.1 400 Bad Request Content-Type: text/plain; charset=utf-8 Sec-Websocket-Version: 13 X-Content-Type-Options: nosniff Date: Thu, 22 Jun 2023 00:57:11 GMT Content-Length: 12 ``` ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10 (version 2004)/Windows Server (version 2004) OS Build: 10.0.19041 Target Name: WINDOWS-C6OJF5R NetBIOS Domain Name: WINDOWS-C6OJF5R NetBIOS Computer Name: WINDOWS-C6OJF5R DNS Domain Name: WINDOWS-C6OJF5R FQDN: WINDOWS-C6OJF5R ``` ---------- **8080:** ``` HTTP/1.1 400 Bad Request Content-Type: text/plain; charset=utf-8 Sec-Websocket-Version: 13 X-Content-Type-Options: nosniff Date: Mon, 26 Jun 2023 03:17:27 GMT Content-Length: 12 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '79.137.203.6']

Name

167.88.15.114

Description

ISP: Nexeon Technologies, Inc. **OS:** None ---------- Hostnames: - jpcloudusa027.nshostserver.net - www.alianneasherman.com - alianneasherman.com ---------- Domains: - nshostserver.net - alianneasherman.com ---------- Services: **21:** ``` 220 FTP Server Ready 530 Login incorrect. 214-The following commands are recognized (* =>'s unimplemented): CWD XCWD CDUP XCUP SMNT* QUIT PORT PASV EPRT EPSV ALLO* RNFR RNTO DELE MDTM RMD XRMD MKD XMKD PWD XPWD SIZE SYST HELP NOOP FEAT OPTS HOST CLNT AUTH CCC* CONF* ENC* MIC* PBSZ PROT TYPE STRU MODE RETR STOR STOU APPE REST ABOR USER PASS ACCT* REIN* LIST NLST STAT SITE MLSD MLST 214 Direct comments to root@167.88.15.114 211-Features: AUTH TLS CCC CLNT EPRT EPSV HOST MDTM MFF modify;UNIX.group;UNIX.mode; MFMT MLST modify*;perm*;size*;type*;unique*;UNIX.group*;UNIX.groupname*;UNIX.mode*;UNIX.owner*; UNIX.ownername*; PBSZ PROT REST STREAM SIZE SSCN TVFS 211 End ``` ---------- **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDUvnqOY7mPbZW2YkTkVfV+xo5JoPU6gQofB9Y7VLmV6rxT 4njJBQy3T/PxyNwQlOgz9M+ +rOEhAvwVwnBIQczL4u1oNVu4eLofSW4ddehV+ZKztaPjQe0QFzcm lz4qz4Dnz3Jf21GWR2cpJRD2rMJ0giwbGzuX5YupBMWt9+qCkPZAsGk7zsnBuHUmXbWMifW40Tpd BFINiuvBeq6zAFJyNl8cK3Ej6dTDArOD6+hPnnfxvQeTyEpXt/oXzafTrOeYFliDouYi6wP4/axP eC2WGURl/i1e/f/uVpaNcDY1O8dvdLJKvrZ79pRwEI1fSjrvKttZuw8OW8v3T5ji7lSF Fingerprint: f9:3a:3b:0a:38:ed:73:b1:a2:dd:db:f1:81:b2:53:c6 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-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-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 aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc 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 ``` ---------- **25:** ``` 220 jpcloudusa027.nshostserver.net InterWorx-CP SMTP Server ESMTP 250-jpcloudusa027.nshostserver.net InterWorx-CP SMTP Server 250-AUTH LOGIN

PLAIN 250-AUTH=LOGIN PLAIN 250-STARTTLS 250-SIZE 20971520 250-PIPELINING 250 8BITMIME ``` ---------- **80:** ``` HTTP/1.1 403 Forbidden Date: Fri, 23 Jun 2023 04:02:53 GMT Server: Apache/2.4.53 (CentOS) Content-Length: 397 Connection: close Content-Type: text/html; charset=iso-8859-1 ``` ---------- **110:** ``` +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE STLS USER SASL . ``` ---------- **443:** ``` HTTP/1.1 200 200 Date: Mon, 03 Jul 2023 06:19:51 GMT Server: Apache/2.4.53 (CentOS) Upgrade: h2 Connection: Upgrade, close Accept-Ranges: bytes ETag: W/"9570-1662023646502" Last-Modified: Thu, 01 Sep 2022 09:14:06 GMT Content-Length: 9570 Content-Type: text/html; charset=UTF-8 ``` HEARTBLEED: 2023/07/03 06:20:47 167.88.15.114:443 - SAFE ---------- **2080:** ``` HTTP/1.1 200 OK Date: Mon, 19 Jun 2023 06:50:41 GMT Server: Apache Set-Cookie: interworx-cp=8ok4ksmhuccnk3626suoa105hk; path=/; secure; HttpOnly X-Interworx-log-id: nosess-p2xi-e6ac-WEB Vary: User-Agent,Accept-Encoding Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 ``` ---------- **2443:** ``` HTTP/1.1 400 Bad Request Date: Thu, 29 Jun 2023 13:42:22 GMT Server: Apache Content-Length: 362 Connection: close Content-Type: text/html; charset=iso-8859-1 ``` ---------- **3306:** ``` MariaDB: Protocol Version: 10 Version: 10.2.44-MariaDB Capabilities: 63486 Server Language: 8 Server Status: 2 Extended Server Capabilities: 33215 Authentication Plugin: mysql_native_password ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '167.88.15.114']

Name

77.105.147.140

Description

ISP: AEZA GROUP Ltd **OS:** None ---------- Hostnames: - picayune-tooth.aeza.network ---------- Domains: - aeza.network ---------- Services: **80:** ``` HTTP/1.1 200 OK Date: Sun, 25 Jun 2023 12:35:39 GMT Server: Apache/2.4.41 (Ubuntu) X-Frame-Options: DENY X-Content-Type-Options: nosniff Access-Control-Allow-Origin: * Access-Control-Allow-Credentials: true Access-

Control-Allow-Methods: GET, POST, OPTIONS Vary: Accept-Encoding Content-Length: 220 Content-Type: text/html; charset=UTF-8 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '77.105.147.140']

Name

afbf62a466552392a4b2c0aa8c51bf3bde84afbe5aa84a2483dc92e906421d0a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'afbf62a466552392a4b2c0aa8c51bf3bde84afbe5aa84a2483dc92e906421d0a']

Malware

Name
Meduza

StixFile

Value
cbc07d45dd4967571f86ae75b120b620b701da11c4ebfa9afcae3a0220527972
1c70f987a0839d11826f053ae90e81a277fa154f5358303fe9a511dbe8b529f2
ddf3604bdfa1e5542cfee4d06a4118214a23f1a65364f44e53e0b68cbfc588ea
f0c730ae57d07440a0de0889db93705c1724f8c3c628ee16a250240cc4f91858
6d8ed1dfcb2d8a9e3c2d51fa106b70a685cbd85569ffabb5692100be75014803
29cf1ba279615a9f4c31d6441dd7c93f5b8a7d95f735c0daa3cc4dbb799f66d4
a73e95fb7ba212f74e0116551ccba73dd2ccba87d8927af29499bba9b3287ea7
91efe60eb46d284c3cfcb584d93bc5b105bf9b376bee761c504598d064b918d4
afbf62a466552392a4b2c0aa8c51bf3bde84afbe5aa84a2483dc92e906421d0a
f575eb5246b5c6b9044ea04610528c040c982904a5fb3dc1909ce2f0ec15c9ef
702abb15d988bba6155dd440f615bbfab9f3c0ed662fc3e64ab1289a1098af98
2ad84bfff7d5257fdeb81b4b52b8e0115f26e8e0cdaa014f9e3084f518aa6149

IPv4-Addr

Value
79.137.203.6
79.137.203.37
89.185.85.245
185.106.94.105
77.105.147.140
79.137.203.39
167.88.15.114
79.137.207.132

Url

Value
http://89.185.85.245

External References

- https://otx.alienvault.com/pulse/64a2f554317bc46cc4bdb6e7
- https://russianpanda.com/2023/06/28/Meduza-Stealer-or-The-Return-of-The-Infamous-Aurora-Stealer/