Feb 23 2024

NETMANAGEIT

Intelligence Report

Doppelgänger | Russia-Aligned Influence Operation Targets Germany

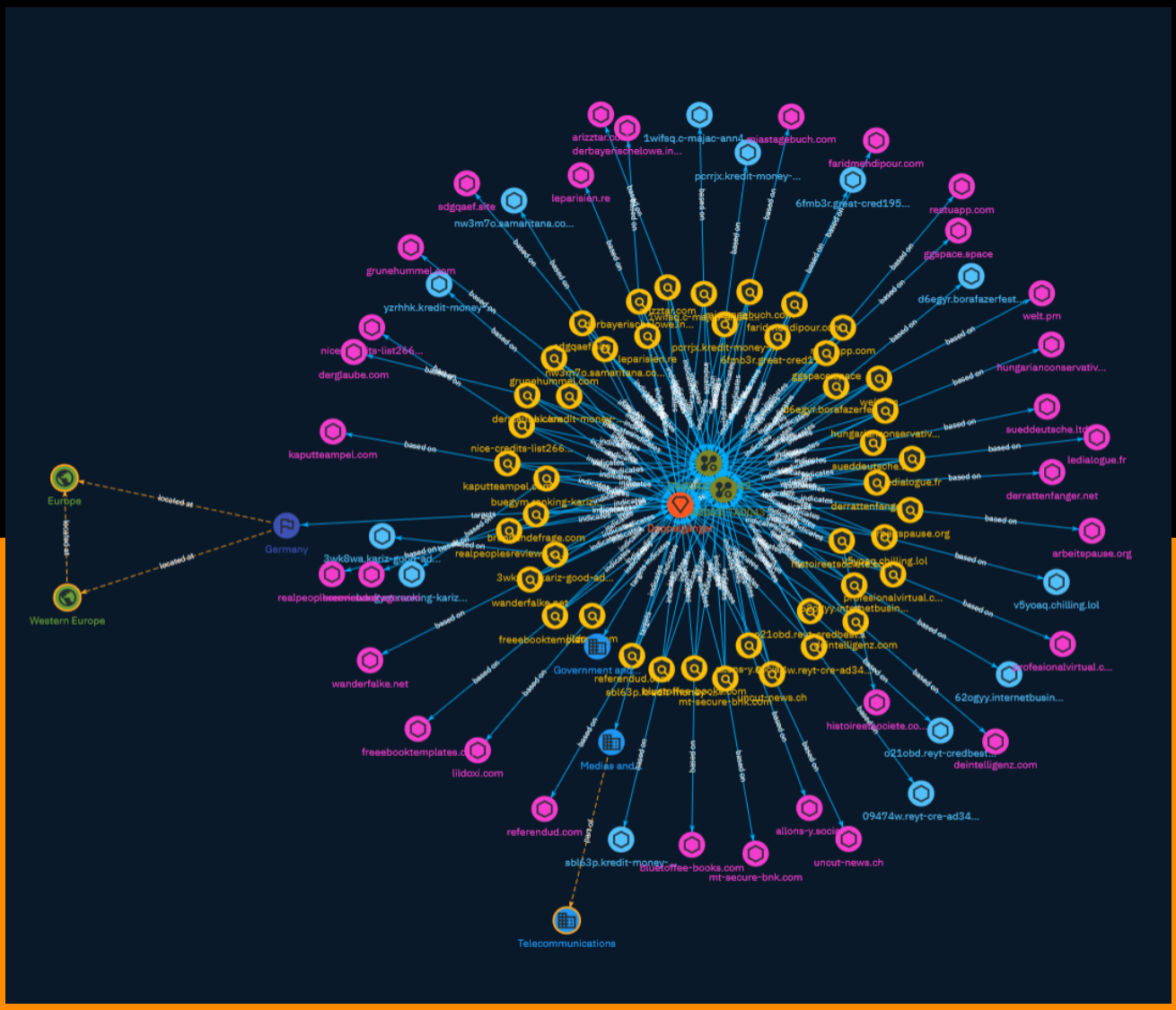

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A suspected Russia-aligned influence operation network named Doppelgänger has been conducting an intensive propaganda and disinformation campaign targeting German audiences. The network exploits topics of socio-economic and geopolitical significance, criticizing the ruling government coalition and its support for Ukraine, likely aiming to influence public opinion before upcoming elections in Germany.

Confidence

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

15 / 100

Content

N/A

Indicator

Name
v5yoaq.chilling.lol
Pattern Type
stix
Pattern
[hostname:value = 'v5yoaq.chilling.lol']
Name
yzrhhk.kredit-money-fun202.buzz
Pattern Type
stix
Pattern
[hostname:value = 'yzrhhk.kredit-money-fun202.buzz']
Name
sbl63p.kredit-money-fun274.buzz

Pattern Type
stix
Pattern
[hostname:value = 'sbl63p.kredit-money-fun274.buzz']
Name
pcrrjx.kredit-money-fun169.buzz
Pattern Type
stix
Pattern
[hostname:value = 'pcrrjx.kredit-money-fun169.buzz']
Name
o21obd.reyt-credbest-mx29.buzz
Pattern Type
stix
Pattern
[hostname:value = 'o21obd.reyt-credbest-mx29.buzz']
Name
nw3m7o.samaritana.com.br

Pattern Type

stix

Pattern

[hostname:value = 'nw3m7o.samaritana.com.br']

Name

d6egyr.borafazerfestaoficial.online

Pattern Type

stix

Pattern

[hostname:value = 'd6egyr.borafazerfestaoficial.online']

Name

buegym.ranking-kariz108.buzz

Pattern Type

stix

Pattern

[hostname:value = 'buegym.ranking-kariz108.buzz']

Name

6fmb3r.great-cred195.buzz

Pattern Type

stix

Pattern

[hostname:value = '6fmb3r.great-cred195.buzz']

Name

62ogyy.internetbusinesslondon.co.uk

Pattern Type

stix

Pattern

[hostname:value = '62ogyy.internetbusinesslondon.co.uk']

Name

3wk8wa.kariz-good-ad10.buzz

Pattern Type

stix

Pattern

[hostname:value = '3wk8wa.kariz-good-ad10.buzz']

Name

09474w.reyt-cre-ad34.buzz

Pattern Type

stix

Pattern

[hostname:value = '09474w.reyt-cre-ad34.buzz']

Name

1wifsq.c-majac-ann4.buzz

Pattern Type

stix

Pattern

[hostname:value = '1wifsq.c-majac-ann4.buzz']

Name

welt.pm

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 1791 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** News - **Domain Age:** {'human': '1 month ago', 'timestamp': 1704988468, 'iso': '2024-01-11T10:54:28-05:00'} - **IPQS: Domain:** welt.de - **IPQS: IP Address:** 104.76.210.205

Pattern Type

stix

Pattern

[domain-name:value = 'welt.pm']

Name

wanderfalke.net

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '12 months ago', 'timestamp': 1677172575, 'iso': '2023-02-23T12:16:15-05:00'} - **IPQS: Domain:** wanderfalke.net - **IPQS: IP Address:** 63.250.43.130

Pattern Type

stix

Pattern

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

Name

sueddeutsche.ltd

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 2828 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** News - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** sueddeutsche.de - **IPQS: IP Address:** 3.163.80.77

Pattern Type

stix

Pattern

[domain-name:value = 'sueddeutsche.ltd']

Name

uncut-news.ch

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 93678 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Business - **Domain Age:** {'human': '37 years ago', 'timestamp': 548549983, 'iso': '1987-05-20T18:59:43-04:00'} - **IPQS: Domain:** uncutnews.ch - **IPQS: IP Address:** 217.26.61.182

Pattern Type

stix

Pattern

[domain-name:value = 'uncut-news.ch']

Name

sdgqaef.site

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False -

Suspicious: True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1701970702, 'iso': '2023-12-07T12:38:22-05:00'} - **IPQS: Domain:** sdgqaef.site - **IPQS: IP Address:** 172.67.140.31

Pattern Type

stix

Pattern

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

Name

restuapp.com

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': '5 years ago', 'timestamp': 1540495412, 'iso': '2018-10-25T15:23:32-04:00'} - **IPQS: Domain:** restuapp.com - **IPQS: IP Address:** 95.213.173.17

Pattern Type

stix

Pattern

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

Name

referendud.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': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** referendud.com - **IPQS: IP Address:** 201.49.135.135

Pattern Type

stix

Pattern

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

Name

realpeoplesreviews.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 139287 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '5 years ago', 'timestamp': 1545574942, 'iso': '2018-12-23T09:22:22-05:00'} - **IPQS: Domain:** realpeoplesreviews.com - **IPQS: IP Address:** 206.188.197.116

Pattern Type

stix

Pattern

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

Name

profesionalvirtual.com

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': '8 years ago', 'timestamp': 1445740081, 'iso': '2015-10-24T22:28:01-04:00'} - **IPQS: Domain:** profesionalvirtual.com - **IPQS: IP Address:** 64.190.113.45

Pattern Type

stix

Pattern

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

Name

nice-credits-list266.buzz

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '10 months ago', 'timestamp': 1683045011, 'iso': '2023-05-02T12:30:11-04:00'} - **IPQS: Domain:** nice-credits-list266.buzz - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'nice-credits-list266.buzz']

Name

miastagebuch.com

Description

- **Unsafe:** False - **Server:** LiteSpeed - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '12 months ago', 'timestamp': 1677571300, 'iso': '2023-02-28T03:01:40-05:00'} - **IPQS: Domain:** miastagebuch.com - **IPQS: IP Address:** 86.104.15.60

Pattern Type

stix

Pattern

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

Name

mt-secure-bnk.com

Description

- **Unsafe:** True - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '11 months ago', 'timestamp': 1679501920, 'iso': '2023-03-22T12:18:40-04:00'} - **IPQS: Domain:** mt-secure-bnk.com - **IPQS: IP Address:** 206.71.148.217

Pattern Type

stix

Pattern

[domain-name:value = 'mt-secure-bnk.com']

Name

lildoxi.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Home & family - **Domain Age:** {'human': '1 year ago', 'timestamp': 1677071948, 'iso': '2023-02-22T08:19:08-05:00'} - **IPQS: Domain:** lildoxi.com - **IPQS: IP Address:** 173.254.29.33

Pattern Type

stix

Pattern

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

Name

leparisien.re

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False -

Suspicious: True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1701439548, 'iso': '2023-12-01T09:05:48-05:00'} - **IPQS: Domain:** leparisien.re - **IPQS: IP Address:** 172.67.166.193

Pattern Type

stix

Pattern

[domain-name:value = 'leparisien.re']

Name

ledialogue.fr

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 year ago', 'timestamp': 1674494418, 'iso': '2023-01-23T12:20:18-05:00'} - **IPQS: Domain:** ledialogue.fr - **IPQS: IP Address:** 104.21.35.9

Pattern Type

stix

Pattern

[domain-name:value = 'ledialogue.fr']

Name

kaputteampel.com

Description

- **Unsafe:** False - **Server:** LiteSpeed - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '8 months ago', 'timestamp': 1688554678, 'iso': '2023-07-05T06:57:58-04:00'} - **IPQS: Domain:** kaputteampel.com - **IPQS: IP Address:** 154.49.138.8

Pattern Type

stix

Pattern

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

Name

hungarianconservative.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** News - **Domain Age:** {'human': '3 years ago', 'timestamp': 1602675566, 'iso': '2020-10-14T07:39:26-04:00'} - **IPQS: Domain:** hungarianconservative.com - **IPQS: IP Address:** 141.193.213.21

Pattern Type

stix

Pattern

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

Name

histoireetsociete.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:** Entertainment - **Domain Age:** {'human': '4 years ago', 'timestamp': 1581356771, 'iso': '2020-02-10T12:46:11-05:00'} - **IPQS: Domain:** histoireetsociete.com - **IPQS: IP Address:** 188.165.4.35

Pattern Type

stix

Pattern

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

Name

grunehummel.com

Description

- **Unsafe:** False - **Server:** LiteSpeed - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '12 months ago', 'timestamp': 1677571339, 'iso': '2023-02-28T03:02:19-05:00'} - **IPQS: Domain:** grunehummel.com - **IPQS: IP Address:** 86.104.15.60

Pattern Type

stix

Pattern

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

Name

ggspace.space

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '5 months ago', 'timestamp': 1696330068, 'iso': '2023-10-03T06:47:48-04:00'} - **IPQS: Domain:** ggspace.space - **IPQS: IP Address:** 172.67.180.148

Pattern Type

stix

Pattern

[domain-name:value = 'ggspace.space']

Name

freeebooktemplates.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': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** freeebooktemplates.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

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

Name

faridmehdipour.com

Description

- **Unsafe:** False - **Server:** hcd - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '8 months ago', 'timestamp': 1686707968, 'iso': '2023-06-13T21:59:28-04:00'} - **IPQS: Domain:** faridmehdipour.com - **IPQS: IP Address:** 84.32.84.115

Pattern Type

stix

Pattern

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

Name

derrattenfanger.net

Description

- **Unsafe:** False - **Server:** LiteSpeed - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False -

Suspicious: False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '12 months ago', 'timestamp': 1677498599, 'iso': '2023-02-27T06:49:59-05:00'} - **IPQS: Domain:** derrattenfanger.net - **IPQS: IP Address:** 89.117.9.58

Pattern Type

stix

Pattern

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

Name

derglaube.com

Pattern Type

stix

Pattern

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

Name

deintelligenz.com

Description

- **Unsafe:** False - **Server:** LiteSpeed - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '8 months ago', 'timestamp': 1688551127, 'iso': '2023-07-05T05:58:47-04:00'} - **IPQS: Domain:** deintelligenz.com - **IPQS: IP Address:** 84.32.84.98

Pattern Type

stix

Pattern

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

Name

derbayerischelowe.info

Description

- **Unsafe:** False - **Server:** LiteSpeed - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '12 months ago', 'timestamp': 1677487059, 'iso': '2023-02-27T03:37:39-05:00'} - **IPQS: Domain:** derbayerischelowe.info - **IPQS: IP Address:** 86.104.15.60

Pattern Type

stix

Pattern

[domain-name:value = 'derbayerischelowe.info']

Name

brennendefrage.com

Description

- **Unsafe:** False - **Server:** LiteSpeed - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False -

Suspicious: False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '12 months ago', 'timestamp': 1677498742, 'iso': '2023-02-27T06:52:22-05:00'} - **IPQS: Domain:** brennendefrage.com - **IPQS: IP Address:** 89.117.9.58

Pattern Type

stix

Pattern

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

Name

bluetoffee-books.com

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': '11 years ago', 'timestamp': 1372801769, 'iso': '2013-07-02T17:49:29-04:00'} - **IPQS: Domain:** bluetoffee-books.com - **IPQS: IP Address:** 64.190.113.45

Pattern Type

stix

Pattern

[domain-name:value = 'bluetoffee-books.com']

Name

arizztar.com

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': '4 years ago', 'timestamp': 1584643763, 'iso': '2020-03-19T14:49:23-04:00'} - **IPQS: Domain:** arizztar.com - **IPQS: IP Address:** 206.188.197.116

Pattern Type

stix

Pattern

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

Name

arbeitspause.org

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '12 months ago', 'timestamp': 1677172557, 'iso': '2023-02-23T12:15:57-05:00'} - **IPQS: Domain:** arbeitspause.org - **IPQS: IP Address:** 63.250.43.131

Pattern Type

stix

Pattern

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

Name
allons-y.social
Pattern Type
stix
Pattern
[domain-name:value = 'allons-y.social']

Intrusion-Set

Name
Doppelgänger

Attack-Pattern

Name
TA0042
ID
TA0042
Name
TA0043
ID
TA0043

Country

Name
Germany

Region

Name
Western Europe

Name
Europe

Sector

Name
Medias and audiovisual
Description
Communication outlets used to deliver information by print, broadcast or Internet and people working in these outlets.
Name
Telecommunications
Description
Private and public entities involved in the production, transport and dissemination of information and communication signals.
Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Hostname

Value
yzrhhk.kredit-money-fun202.buzz
v5yoaq.chilling.lol
sbl63p.kredit-money-fun274.buzz
pcrrjx.kredit-money-fun169.buzz
o21obd.reyt-credbest-mx29.buzz
nw3m7o.samaritana.com.br
d6egyr.borafazerfestaoficial.online
buegym.ranking-kariz108.buzz
6fmb3r.great-cred195.buzz
62ogyy.internetbusinesslondon.co.uk
3wk8wa.kariz-good-ad10.buzz
1wifsq.c-majac-ann4.buzz
09474w.reyt-cre-ad34.buzz

Domain-Name

Value
wanderfalke.net
welt.pm
uncut-news.ch
sdgqaef.site
sueddeutsche.ltd
referendud.com
restuapp.com
realpeoplesreviews.com
nice-credits-list266.buzz
profesionalvirtual.com
mt-secure-bnk.com
miastagebuch.com
lildoxi.com

leparisien.re

ledialogue.fr

kaputteampel.com

hungarianconservative.com

histoireetsociete.com

grunehummel.com

ggspace.space

freeebooktemplates.com

faridmehdipour.com

derrattenfanger.net

derglaube.com

derbayerischelowe.info

deintelligenz.com

brennendefrage.com

arbeitspause.org

bluetoffee-books.com

arizztar.com

allons-y.social

External References

- https://www.sentinelone.com/labs/doppelganger-russia-aligned-influence-operation-targets-germany/
- https://otx.alienvault.com/pulse/65d85ad1c949dde495a432b4