Mar 06 2024

NETMANAGEIT

Intelligence Report

Deep fake connected to Russian cyberscam network

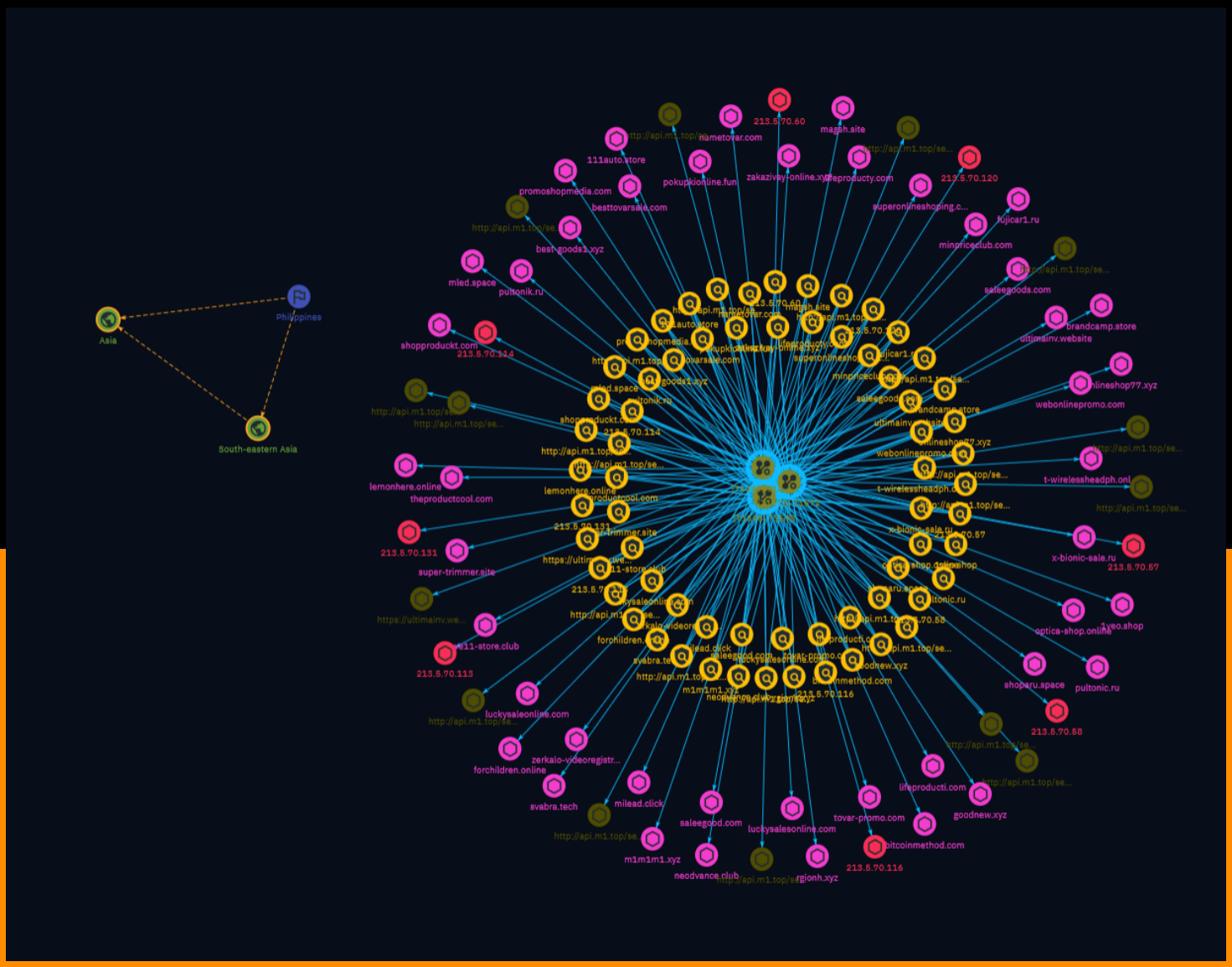

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A deep fake video of Maria Ressa promoting a crypto-currency scam was released in early February 2024. The video was hosted on a domain that contained links to a Russian cyberscam network. Metadata analysis revealed Russian influence behind the creation of the deep fake and fake news articles designed to discredit Ressa.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

zerkalo-videoregistrator-gps.ru

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': '8 minutes ago', 'timestamp': 1709738761, 'iso': '2024-03-06T10:26:01-05:00'} - **IPQS: Domain:** zerkalo-videoregistrator-gps.ru - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'zerkalo-videoregistrator-gps.ru']

Name

zakazivay-online.xyz

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': '8

minutes ago', 'timestamp': 1709738761, 'iso': '2024-03-06T10:26:01-05:00'} - **IPQS: Domain:** zakazivay-online.xyz - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'zakazivay-online.xyz']

Name

x-bionic-sale.ru

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': '1 year ago', 'timestamp': 1667919836, 'iso': '2022-11-08T10:03:56-05:00'} - **IPQS: Domain:** x-bionic-sale.ru - **IPQS: IP Address:** 185.4.75.144

Pattern Type

stix

Pattern

[domain-name:value = 'x-bionic-sale.ru']

Name

we11-store.club

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': '8 minutes ago', 'timestamp': 1709738759, 'iso': '2024-03-06T10:25:59-05:00'} - **IPQS: Domain:** we11-store.club - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'we11-store.club']

Name

ultimainv.website

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': '2 months ago', 'timestamp': 1704914392, 'iso': '2024-01-10T14:19:52-05:00'} - **IPQS: Domain:** ultimainv.website - **IPQS: IP Address:** 104.21.94.190

Pattern Type

stix

Pattern

[domain-name:value = 'ultimainv.website']

Name

tovar-promo.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 865516 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Missing Content - **Domain Age:** {'human': '5 years ago', 'timestamp': 1563461170, 'iso': '2019-07-18T10:46:10-04:00'} - **IPQS: Domain:** tovar-promo.com - **IPQS: IP Address:** 213.5.70.113

Pattern Type

stix

Pattern

[domain-name:value = 'tovar-promo.com']

Name

theproductcool.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 844855 - **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': 1564672246, 'iso': '2019-08-01T11:10:46-04:00'} - **IPQS: Domain:** theproductcool.com - **IPQS: IP Address:** 213.5.70.113

Pattern Type

stix

Pattern

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

Name

t-wirelessheadph.online

Description

- **Unsafe:** False - **Server:** LiteSpeed - **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': 1689439299, 'iso': '2023-07-15T12:41:39-04:00'} - **IPQS: Domain:** t-wirelessheadph.online - **IPQS: IP Address:** 45.84.204.161

Pattern Type

stix

Pattern

[domain-name:value = 't-wirelessheadph.online']

Name

svabra.tech

Description

- **Unsafe:** False - **Server:** LiteSpeed - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '7 months ago', 'timestamp': 1690532837, 'iso': '2023-07-28T04:27:17-04:00'} - **IPQS: Domain:** svabra.tech - **IPQS: IP Address:** 45.84.204.161

Pattern Type

stix

Pattern

[domain-name:value = 'svabra.tech']

Name

super-trimmer.site

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': '8 months ago', 'timestamp': 1689424502, 'iso': '2023-07-15T08:35:02-04:00'} - **IPQS: Domain:** super-trimmer.site - **IPQS: IP Address:** 185.104.45.199

Pattern Type

stix

Pattern

[domain-name:value = 'super-trimmer.site']

Name

superonlineshoping.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Business - **Domain Age:** {'human': '5 years ago',

'timestamp': 1565248896, 'iso': '2019-08-08T03:21:36-04:00'} - **IPQS: Domain:** superonlineshoping.com - **IPQS: IP Address:** 213.5.70.57

Pattern Type

stix

Pattern

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

Name

shoparu.space

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': '1 year ago', 'timestamp': 1674129534, 'iso': '2023-01-19T06:58:54-05:00'} - **IPQS: Domain:** shoparu.space - **IPQS: IP Address:** 213.5.70.113

Pattern Type

stix

Pattern

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

Name

saleegoods.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 772533 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Missing Content - **Domain Age:** {'human': '5 years ago', 'timestamp': 1559730960, 'iso': '2019-06-05T06:36:00-04:00'} - **IPQS: Domain:** saleegoods.com - **IPQS: IP Address:** 213.5.70.113

Pattern Type

stix

Pattern

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

Name

saleegood.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': '7 months ago', 'timestamp': 1692619827, 'iso': '2023-08-21T08:10:27-04:00'} - **IPQS: Domain:** saleegood.com - **IPQS: IP Address:** 213.5.70.131

Pattern Type

stix

Pattern

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

Name

pultonik.ru

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': '2 years ago', 'timestamp': 1636485024, 'iso': '2021-11-09T14:10:24-05:00'} - **IPQS: Domain:** pultonik.ru - **IPQS: IP Address:** 185.114.247.102

Pattern Type

stix

Pattern

[domain-name:value = 'pultonik.ru']

Name

promoshopmedia.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 620585 - **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': 1565248904, 'iso': '2019-08-08T03:21:44-04:00'} - **IPQS: Domain:** promoshopmedia.com - **IPQS: IP Address:** 213.5.70.113

Pattern Type

stix

Pattern

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

Name

pultonic.ru

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': '2 years ago', 'timestamp': 1642167301, 'iso': '2022-01-14T08:35:01-05:00'} - **IPQS: Domain:** pultonic.ru - **IPQS: IP Address:** 185.114.247.102

Pattern Type

stix

Pattern

[domain-name:value = 'pultonic.ru']

Name

pokupkionline.fun

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': '9 months ago', 'timestamp': 1685898667, 'iso': '2023-06-04T13:11:07-04:00'} - **IPQS: Domain:** pokupkionline.fun - **IPQS: IP Address:** 213.5.70.114

Pattern Type

stix

Pattern

[domain-name:value = 'pokupkionline.fun']

Name

nametovar.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 294844 - **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': 1564504036, 'iso': '2019-07-30T12:27:16-04:00'} - **IPQS: Domain:** nametovar.com - **IPQS: IP Address:** 213.5.70.113

Pattern Type

stix

Pattern

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

Name

neodvance.club

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': 1561547562, 'iso': '2019-06-26T07:12:42-04:00'} - **IPQS: Domain:** neodvance.club - **IPQS: IP Address:** 213.5.70.57

Pattern Type

stix

Pattern

[domain-name:value = 'neodvance.club']

Name

minpriceclub.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': '10 months ago', 'timestamp': 1683580301, 'iso': '2023-05-08T17:11:41-04:00'} - **IPQS: Domain:** minpriceclub.com - **IPQS: IP Address:** 213.5.70.116

Pattern Type

stix

Pattern

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

Name

milead.click

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': '7 minutes ago', 'timestamp': 1709738738, 'iso': '2024-03-06T10:25:38-05:00'} - **IPQS: Domain:** milead.click - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'milead.click']

Name

luckysalesonline.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': '7 months ago', 'timestamp': 1692619834, 'iso': '2023-08-21T08:10:34-04:00'} - **IPQS: Domain:** luckysalesonline.com - **IPQS: IP Address:** 213.5.70.131

Pattern Type

stix

Pattern

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

Name

magsh.site

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': '1 year ago', 'timestamp': 1674129540, 'iso': '2023-01-19T06:59:00-05:00'} - **IPQS: Domain:** magsh.site - **IPQS: IP Address:** 213.5.70.113

Pattern Type

stix

Pattern

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

Name

luckysaleonline.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 325157 - **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': 1565192631, 'iso': '2019-08-07T11:43:51-04:00'} - **IPQS: Domain:** luckysaleonline.com - **IPQS: IP Address:** 213.5.70.113

Pattern Type

stix

Pattern

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

Name

lifeproducty.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': '7 months ago', 'timestamp': 1692619837, 'iso': '2023-08-21T08:10:37-04:00'} - **IPQS: Domain:** lifeproducty.com - **IPQS: IP Address:** 213.5.70.131

Pattern Type

stix

Pattern

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

Name

lifeproducti.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 280321 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Business - **Domain Age:** {'human': '5 years ago', 'timestamp': 1559726711, 'iso': '2019-06-05T05:25:11-04:00'} - **IPQS: Domain:** lifeproducti.com - **IPQS: IP Address:** 213.5.70.113

Pattern Type

stix

Pattern

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

Name

lemonhere.online

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': 1683798086, 'iso': '2023-05-11T05:41:26-04:00'} - **IPQS: Domain:** lemonhere.online - **IPQS: IP Address:** 213.5.70.114

Pattern Type

stix

Pattern

[domain-name:value = 'lemonhere.online']

Name

fujicar1.ru

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': '2 years ago',

'timestamp': 1641405301, 'iso': '2022-01-05T12:55:01-05:00'} - **IPQS: Domain:** fujicar1.ru - **IPQS: IP Address:** 185.114.247.102

Pattern Type

stix

Pattern

[domain-name:value = 'fujicar1.ru']

Name

bitcoinmethod.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Careers - **Domain Age:** {'human': '8 years ago', 'timestamp': 1471292222, 'iso': '2016-08-15T16:17:02-04:00'} - **IPQS: Domain:** bitcoinmethod.com - **IPQS: IP Address:** 104.21.58.249

Pattern Type

stix

Pattern

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

Name

besttovarsale.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 200405 - **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': 1564576912, 'iso': '2019-07-31T08:41:52-04:00'} - **IPQS: Domain:** besttovarsale.com - **IPQS: IP Address:** 213.5.70.113

Pattern Type

stix

Pattern

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

Name

1veo.shop

Description

- **Unsafe:** False - **Server:** LiteSpeed - **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 months ago', 'timestamp': 1681977160, 'iso': '2023-04-20T03:52:40-04:00'} - **IPQS: Domain:** 1veo.shop - **IPQS: IP Address:** 45.84.204.161

Pattern Type

stix

Pattern

[domain-name:value = '1veo.shop']

Name

https://ultimainv.website/

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': '2 months ago', 'timestamp': 1704914392, 'iso': '2024-01-10T14:19:52-05:00'} - **IPQS: Domain:** ultimainv.website - **IPQS: IP Address:** 104.21.94.190

Pattern Type

stix

Pattern

[url:value = 'https://ultimainv.website/']

Name

http://api.m1.top/send_order/?ref=995399

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Computers & internet - **Domain Age:** {'human': '6 minutes ago', 'timestamp': 1709738715, 'iso': '2024-03-06T10:25:15-05:00'} - **IPQS: Domain:** api.m1.top - **IPQS: IP Address:** 185.203.72.22

Pattern Type

stix

Pattern

[url:value = 'http://api.m1.top/send_order/?ref=995399']

Name

http://api.m1.top/send_order/?ref=990912

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Computers & internet - **Domain Age:** {'human': '6 minutes ago', 'timestamp': 1709738715, 'iso': '2024-03-06T10:25:15-05:00'} - **IPQS: Domain:** api.m1.top - **IPQS: IP Address:** 185.203.72.22

Pattern Type

stix

Pattern

[url:value = 'http://api.m1.top/send_order/?ref=990912']

Name

http://api.m1.top/send_order/?ref=980800

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Computers & internet - **Domain Age:** {'human': '5 minutes ago', 'timestamp': 1709738715, 'iso': '2024-03-06T10:25:15-05:00'} - **IPQS: Domain:** api.m1.top - **IPQS: IP Address:** 185.203.72.22

Pattern Type

stix

Pattern

[url:value = 'http://api.m1.top/send_order/?ref=980800']

Name

http://api.m1.top/send_order/?ref=976966

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Computers & internet - **Domain Age:** {'human': '5 minutes ago', 'timestamp': 1709738715, 'iso': '2024-03-06T10:25:15-05:00'} - **IPQS: Domain:** api.m1.top - **IPQS: IP Address:** 185.203.72.22

Pattern Type

stix

Pattern

[url:value = 'http://api.m1.top/send_order/?ref=976966']

Name

http://api.m1.top/send_order/?ref=970507

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Computers & internet - **Domain Age:** {'human': '5

minutes ago', 'timestamp': 1709738715, 'iso': '2024-03-06T10:25:15-05:00'} - **IPQS: Domain:** api.m1.top - **IPQS: IP Address:** 185.203.72.22

Pattern Type

stix

Pattern

[url:value = 'http://api.m1.top/send_order/?ref=970507']

Name

http://api.m1.top/send_order/?ref=965842

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Computers & internet - **Domain Age:** {'human': '5 minutes ago', 'timestamp': 1709738715, 'iso': '2024-03-06T10:25:15-05:00'} - **IPQS: Domain:** api.m1.top - **IPQS: IP Address:** 185.203.72.22

Pattern Type

stix

Pattern

[url:value = 'http://api.m1.top/send_order/?ref=965842']

Name

http://api.m1.top/send_order/?ref=863220

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Computers & internet - **Domain Age:** {'human': '5 minutes ago', 'timestamp': 1709738715, 'iso': '2024-03-06T10:25:15-05:00'} - **IPQS: Domain:** api.m1.top - **IPQS: IP Address:** 185.203.72.22

Pattern Type

stix

Pattern

[url:value = 'http://api.m1.top/send_order/?ref=863220']

Name

http://api.m1.top/send_order/?ref=955398

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Computers & internet - **Domain Age:** {'human': '5 minutes ago', 'timestamp': 1709738715, 'iso': '2024-03-06T10:25:15-05:00'} - **IPQS: Domain:** api.m1.top - **IPQS: IP Address:** 185.203.72.22

Pattern Type

stix

Pattern

[url:value = 'http://api.m1.top/send_order/?ref=955398']

Name

http://api.m1.top/send_order/?ref=939454

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Computers & internet - **Domain Age:** {'human': '5 minutes ago', 'timestamp': 1709738715, 'iso': '2024-03-06T10:25:15-05:00'} - **IPQS: Domain:** api.m1.top - **IPQS: IP Address:** 185.203.72.22

Pattern Type

stix

Pattern

[url:value = 'http://api.m1.top/send_order/?ref=939454']

Name

http://api.m1.top/send_order/?ref=776256

Pattern Type

stix

Pattern

[url:value = 'http://api.m1.top/send_order/?ref=776256']

Name

http://api.m1.top/send_order/?ref=67558

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Computers & internet - **Domain Age:** {'human': '4 minutes ago', 'timestamp': 1709738715, 'iso': '2024-03-06T10:25:15-05:00'} - **IPQS: Domain:** api.m1.top - **IPQS: IP Address:** 185.203.72.22

Pattern Type

stix

Pattern

[url:value = 'http://api.m1.top/send_order/?ref=67558']

Name

http://api.m1.top/send_order/?ref=257453

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Computers & internet - **Domain Age:** {'human': '4 minutes ago', 'timestamp': 1709738715, 'iso': '2024-03-06T10:25:15-05:00'} - **IPQS: Domain:** api.m1.top - **IPQS: IP Address:** 185.203.72.22

Pattern Type

stix

Pattern

[url:value = 'http://api.m1.top/send_order/?ref=257453']

Name

http://api.m1.top/send_order/?ref=253692

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Computers & internet - **Domain Age:** {'human': '4 minutes ago', 'timestamp': 1709738715, 'iso': '2024-03-06T10:25:15-05:00'} - **IPQS: Domain:** api.m1.top - **IPQS: IP Address:** 185.203.72.22

Pattern Type

stix

Pattern

[url:value = 'http://api.m1.top/send_order/?ref=253692']

Name

213.5.70.60

Description

- **Zip Code:** N/A - **ISP:** AltusHost - **ASN:** 51430 - **Organization:** AltusHost - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** nld-net-ip.as51430.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:** NL - **Region:** Noord-Holland - **City:** Amsterdam - **Latitude:** 52.38 - **Longitude:** 4.9

Pattern Type

stix

Pattern

[ipv4-addr:value = '213.5.70.60']

Name

213.5.70.58

Description

- **Zip Code:** N/A - **ISP:** AltusHost - **ASN:** 51430 - **Organization:** AltusHost - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** nld-net-ip.as51430.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:** NL - **Region:** Noord-Holland - **City:** Amsterdam - **Latitude:** 52.38 - **Longitude:** 4.9

Pattern Type

stix

Pattern

[ipv4-addr:value = '213.5.70.58']

Name

213.5.70.131

Description

- **Zip Code:** N/A - **ISP:** AltusHost - **ASN:** 51430 - **Organization:** AltusHost - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** nld-net-ip.as51430.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:** NL - **Region:** Noord-Holland - **City:** Amsterdam - **Latitude:** 52.38 - **Longitude:** 4.9

Pattern Type

stix

Pattern

[ipv4-addr:value = '213.5.70.131']

Name

213.5.70.120

Description

- **Zip Code:** N/A - **ISP:** AltusHost - **ASN:** 51430 - **Organization:** AltusHost - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** nld-net-ip.as51430.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:** NL - **Region:** Noord-Holland - **City:** Amsterdam - **Latitude:** 52.38 - **Longitude:** 4.9

Pattern Type

stix

Pattern

[ipv4-addr:value = '213.5.70.120']

Name

213.5.70.116

Description

- **Zip Code:** N/A - **ISP:** AltusHost - **ASN:** 51430 - **Organization:** AltusHost - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** ff.owncustoms.com - **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:** NL - **Region:** Noord-Holland - **City:** Amsterdam - **Latitude:** 52.38 - **Longitude:** 4.9

Pattern Type

stix

Pattern

[ipv4-addr:value = '213.5.70.116']

Name

213.5.70.114

Description

- **Zip Code:** N/A - **ISP:** AltusHost - **ASN:** 51430 - **Organization:** AltusHost - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** jh.owncustoms.com - **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:** NL - **Region:** Noord-Holland - **City:** Amsterdam - **Latitude:** 52.38 - **Longitude:** 4.9

Pattern Type

stix

Pattern

[ipv4-addr:value = '213.5.70.114']

Name

213.5.70.57

Description

- **Zip Code:** N/A - **ISP:** AltusHost - **ASN:** 51430 - **Organization:** AltusHost - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** nld-net-ip.as51430.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:** NL - **Region:** Noord-Holland - **City:** Amsterdam - **Latitude:** 52.38 - **Longitude:** 4.9

Pattern Type

stix

Pattern

[ipv4-addr:value = '213.5.70.57']

Name

213.5.70.113

Description

- **Zip Code:** N/A - **ISP:** AltusHost - **ASN:** 51430 - **Organization:** AltusHost - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** owncustoms.com - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** NL - **Region:** Noord-Holland - **City:** Amsterdam - **Latitude:** 52.38 - **Longitude:** 4.9

Pattern Type

stix

Pattern

[ipv4-addr:value = '213.5.70.113']

Name

mled.space

Description

- **Unsafe:** True - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Phishing - **Domain Age:** {'human': '2 years ago', 'timestamp': 1657411033, 'iso': '2022-07-09T19:57:13-04:00'} - **IPQS: Domain:** mled.space - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

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

Name

optica-shop.online

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

minutes ago', 'timestamp': 1709738710, 'iso': '2024-03-06T10:25:10-05:00'} - **IPQS: Domain:** optica-shop.online - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'optica-shop.online']

Name

forchildren.online

Description

- **Unsafe:** False - **Server:** Google Fro - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '1 year ago', 'timestamp': 1677444914, 'iso': '2023-02-26T15:55:14-05:00'} - **IPQS: Domain:** forchildren.online - **IPQS: IP Address:** 35.186.223.180

Pattern Type

stix

Pattern

[domain-name:value = 'forchildren.online']

Name

brandcamp.store

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': '8 months ago', 'timestamp': 1689694803, 'iso': '2023-07-18T11:40:03-04:00'} - **IPQS: Domain:** brandcamp.store - **IPQS: IP Address:** 185.104.45.199

Pattern Type

stix

Pattern

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

Name

rgionh.xyz

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 minutes ago', 'timestamp': 1709738708, 'iso': '2024-03-06T10:25:08-05:00'} - **IPQS: Domain:** rgionh.xyz - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'rgionh.xyz']

Name

best-goods1.xyz

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': '3 minutes ago', 'timestamp': 1709738707, 'iso': '2024-03-06T10:25:07-05:00'} - **IPQS: Domain:** best-goods1.xyz - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'best-goods1.xyz']

Name

onlineshop77.xyz

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 402585 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 minutes ago', 'timestamp': 1709738706, 'iso': '2024-03-06T10:25:06-05:00'} - **IPQS: Domain:** onlineshop77.xyz - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'onlineshop77.xyz']

Name

m1m1m1.xyz

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 minutes ago', 'timestamp': 1709738706, 'iso': '2024-03-06T10:25:06-05:00'} - **IPQS: Domain:** m1m1m1.xyz - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'm1m1m1.xyz']

Name

111auto.store

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': '2 minutes ago', 'timestamp': 1709738706, 'iso': '2024-03-06T10:25:06-05:00'} - **IPQS: Domain:** 111auto.store - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = '111auto.store']

Name

goodnew.xyz

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': '2 minutes ago', 'timestamp': 1709738706, 'iso': '2024-03-06T10:25:06-05:00'} - **IPQS: Domain:** goodnew.xyz - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'goodnew.xyz']

Name

shopproduckt.com

Description

- **Unsafe:** True - **Server:** - **Domain Rank:** 640262 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Phishing - **Domain Age:** {'human':

'5 years ago', 'timestamp': 1559308828, 'iso': '2019-05-31T09:20:28-04:00'} - **IPQS: Domain:** shopproduckt.com - **IPQS: IP Address:** 213.5.70.113

Pattern Type

stix

Pattern

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

Name

webonlinepromo.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 966508 - **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': 1565203290, 'iso': '2019-08-07T14:41:30-04:00'} - **IPQS: Domain:** webonlinepromo.com - **IPQS: IP Address:** 213.5.70.113

Pattern Type

stix

Pattern

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

Attack-Pattern

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

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

T1572

ID

T1572

Description

Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection/network filtering and/or enable access to otherwise unreachable systems. Tunneling involves explicitly encapsulating a protocol within another. This behavior may conceal malicious traffic by blending in with existing traffic and/or provide an outer layer of encryption (similar to a VPN). Tunneling could also enable routing of network packets that would otherwise not reach their intended destination, such as SMB, RDP, or other traffic that would be filtered by network appliances or not routed over the Internet. There are various means to encapsulate a protocol within another protocol. For example, adversaries may perform SSH tunneling (also known as SSH port forwarding), which involves forwarding arbitrary data over an encrypted SSH tunnel. (Citation: SSH Tunneling) [Protocol Tunneling](https://attack.mitre.org/techniques/T1572) may also be abused by adversaries during [Dynamic Resolution](https://attack.mitre.org/techniques/T1568). Known as DNS over HTTPS (DoH), queries to resolve C2 infrastructure may be encapsulated within encrypted HTTPS packets.(Citation: BleepingComp Godlua JUL19) Adversaries may also leverage [Protocol Tunneling](https://attack.mitre.org/techniques/T1572) in conjunction with [Proxy](https://attack.mitre.org/techniques/T1090)

and/or [Protocol Impersonation](https://attack.mitre.org/techniques/T1001/003) to further conceal C2 communications and infrastructure.

Country

Name
Philippines

Region

Name
South-eastern Asia

Name
Asia

Domain-Name

Value
zerkalo-videoregistrator-gps.ru
zakazivay-online.xyz
x-bionic-sale.ru
we11-store.club
ultimainv.website
tovar-promo.com
theproductcool.com
t-wirelessheadph.online
svabra.tech
superonlineshoping.com
shoparu.space
super-trimmer.site
saleegoods.com

saleegood.com

pultonik.ru

pultonic.ru

promoshopmedia.com

pokupkionline.fun

neodvance.club

nametovar.com

minpriceclub.com

milead.click

magsh.site

luckysalesonline.com

luckysaleonline.com

lifeproducty.com

lifeproducti.com

lemonhere.online

fujicar1.ru

bitcoinmethod.com

besttovarsale.com

1veo.shop
mled.space
optica-shop.online
forchildren.online
brandcamp.store
rgionh.xyz
best-goods1.xyz
m1m1m1.xyz
111auto.store
onlineshop77.xyz
goodnew.xyz
shopproduckt.com
webonlinepromo.com

Url

Value
https://ultimainv.website/
http://api.m1.top/send_order/?ref=995399
http://api.m1.top/send_order/?ref=990912
http://api.m1.top/send_order/?ref=980800
http://api.m1.top/send_order/?ref=976966
http://api.m1.top/send_order/?ref=970507
http://api.m1.top/send_order/?ref=965842
http://api.m1.top/send_order/?ref=955398
http://api.m1.top/send_order/?ref=939454
http://api.m1.top/send_order/?ref=863220
http://api.m1.top/send_order/?ref=776256
http://api.m1.top/send_order/?ref=67558
http://api.m1.top/send_order/?ref=257453

http://api.m1.top/send_order/?ref=253692

IPv4-Addr

Value
213.5.70.60
213.5.70.58
213.5.70.131
213.5.70.120
213.5.70.116
213.5.70.114
213.5.70.57
213.5.70.113

External References

- https://www.qurium.org/alerts/philippines/deep-fake-video-of-maria-ressa-connected-to-cyberscam-network-in-russia/
- https://otx.alienvault.com/pulse/65e8893540292ac6c7e080ff