Mar 05 2024

NETMANAGEIT

Intelligence Report

Spyware Operators Rebuild Multi-Tier Infrastructure to Target Mobile Devices

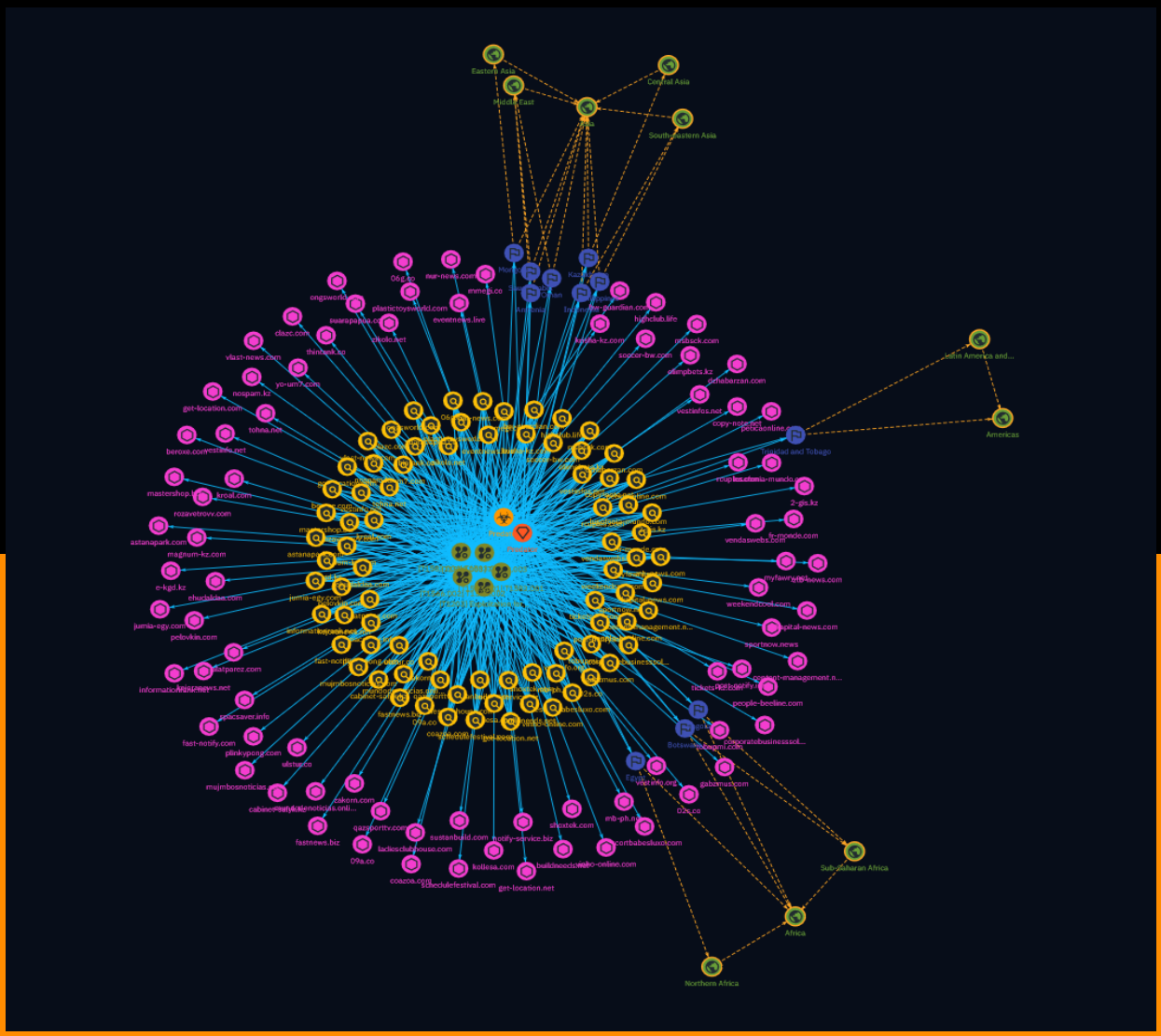

Table of contents

Overview

Entities

Observables

External References

Overview

Description

New research reveals that operators of the Predator spyware have rebuilt a multi-tier infrastructure targeting mobile devices in at least eleven countries. The spyware is marketed for counterterrorism but often used against civil society. Technical analysis identified new delivery domains and servers still active after public disclosures in 2023. Users should follow security best practices like updates, lockdown mode, and separating personal and corporate devices.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

zikolo.net

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1699623734, 'iso': '2023-11-10T08:42:14-05:00'} - **IPQS: Domain:** zikolo.net - **IPQS: IP Address:** 193.168.143.116

Pattern Type

stix

Pattern

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

Name

zakorn.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4

months ago', 'timestamp': 1699531106, 'iso': '2023-11-09T06:58:26-05:00'} - **IPQS: Domain:** zakorn.com - **IPQS: IP Address:** 193.168.143.111

Pattern Type

stix

Pattern

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

Name

yo-um7.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': '3 months ago', 'timestamp': 1701178339, 'iso': '2023-11-28T08:32:19-05:00'} - **IPQS: Domain:** yo-um7.com - **IPQS: IP Address:** 185.130.46.202

Pattern Type

stix

Pattern

[domain-name:value = 'yo-um7.com']

Name

weekendcool.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** True - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1700227464, 'iso': '2023-11-17T08:24:24-05:00'} - **IPQS: Domain:** weekendcool.com - **IPQS: IP Address:** 185.113.8.83

Pattern Type

stix

Pattern

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

Name

walatparez.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1701945858, 'iso': '2023-12-07T05:44:18-05:00'} - **IPQS: Domain:** walatparez.com - **IPQS: IP Address:** 193.233.161.137

Pattern Type

stix

Pattern

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

Name

vestinfos.net

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1702288781, 'iso': '2023-12-11T04:59:41-05:00'} - **IPQS: Domain:** vestinfos.net - **IPQS: IP Address:** 185.130.45.34

Pattern Type

stix

Pattern

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

Name

vestinfo.org

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1702301422, 'iso': '2023-12-11T08:30:22-05:00'} - **IPQS: Domain:** vestinfo.org - **IPQS: IP Address:** 79.141.175.146

Pattern Type

stix

Pattern

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

Name

vestinfo.net

Pattern Type

stix

Pattern

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

Name

vendaswebs.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1700058610, 'iso': '2023-11-15T09:30:10-05:00'} - **IPQS: Domain:** vendaswebs.com - **IPQS: IP Address:** 217.70.184.50

Pattern Type

stix

Pattern

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

Name

tohna.net

Pattern Type

stix

Pattern

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

Name

ulstur.co

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1703244987, 'iso': '2023-12-22T06:36:27-05:00'} - **IPQS: Domain:** ulstur.co - **IPQS: IP Address:** 84.247.51.18

Pattern Type

stix

Pattern

[domain-name:value = 'ulstur.co']

Name

tobupmi.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** True - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1699957753, 'iso': '2023-11-14T05:29:13-05:00'} - **IPQS: Domain:** tobupmi.com - **IPQS: IP Address:** 193.233.161.163

Pattern Type

stix

Pattern

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

Name

thintank.co

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1698140179, 'iso': '2023-10-24T05:36:19-04:00'} - **IPQS: Domain:** thintank.co - **IPQS: IP Address:** 5.255.88.172

Pattern Type

stix

Pattern

[domain-name:value = 'thintank.co']

Name

tickets-kz.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1702043425, 'iso': '2023-12-08T08:50:25-05:00'} - **IPQS: Domain:** tickets-kz.com - **IPQS: IP Address:** 45.86.163.77

Pattern Type

stix

Pattern

[domain-name:value = 'tickets-kz.com']

Name

sustanbuild.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': '3 months ago', 'timestamp': 1700753650, 'iso': '2023-11-23T10:34:10-05:00'} - **IPQS: Domain:** sustanbuild.com - **IPQS: IP Address:** 193.29.104.5

Pattern Type

stix

Pattern

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

Name

suarapapua.co

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1701378270, 'iso': '2023-11-30T16:04:30-05:00'} - **IPQS: Domain:** suarapapua.co - **IPQS: IP Address:** 158.58.172.3

Pattern Type

stix

Pattern

[domain-name:value = 'suarapapua.co']

Name

sportnow.news

Description

- **Unsafe:** False - **Server:** Apache - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1699607910, 'iso': '2023-11-10T04:18:30-05:00'} - **IPQS: Domain:** sportnow.news - **IPQS: IP Address:** 185.113.8.67

Pattern Type

stix

Pattern

[domain-name:value = 'sportnow.news']

Name

spacsaver.info

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': '3 months ago', 'timestamp': 1701270276, 'iso': '2023-11-29T10:04:36-05:00'} - **IPQS: Domain:** spacsaver.info - **IPQS: IP Address:** 45.148.244.5

Pattern Type

stix

Pattern

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

Name

soccer-bw.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago',

'timestamp': 1700352027, 'iso': '2023-11-18T19:00:27-05:00'} - **IPQS: Domain:** soccer-bw.com - **IPQS: IP Address:** 185.130.46.165

Pattern Type

stix

Pattern

[domain-name:value = 'soccer-bw.com']

Name

shoxtek.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': '3 months ago', 'timestamp': 1700740166, 'iso': '2023-11-23T06:49:26-05:00'} - **IPQS: Domain:** shoxtek.com - **IPQS: IP Address:** 46.30.190.98

Pattern Type

stix

Pattern

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

Name

rozavetrovv.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1702479673, 'iso': '2023-12-13T10:01:13-05:00'} - **IPQS: Domain:** rozavetrovv.com - **IPQS: IP Address:** 5.39.221.48

Pattern Type

stix

Pattern

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

Name

rcuples.com

Pattern Type

stix

Pattern

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

Name

qazsporttv.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago',

'timestamp': 1702479701, 'iso': '2023-12-13T10:01:41-05:00'} - **IPQS: Domain:** qazsporttv.com - **IPQS: IP Address:** 185.117.91.237

Pattern Type

stix

Pattern

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

Name

plastictoysworld.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1700582983, 'iso': '2023-11-21T11:09:43-05:00'} - **IPQS: Domain:** plastictoysworld.com - **IPQS: IP Address:** 185.130.227.88

Pattern Type

stix

Pattern

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

Name

people-beeline.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1702479648, 'iso': '2023-12-13T10:00:48-05:00'} - **IPQS: Domain:** people-beeline.com - **IPQS: IP Address:** 5.39.221.47

Pattern Type

stix

Pattern

[domain-name:value = 'people-beeline.com']

Name

pelovkin.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1701096877, 'iso': '2023-11-27T09:54:37-05:00'} - **IPQS: Domain:** pelovkin.com - **IPQS: IP Address:** 185.117.91.165

Pattern Type

stix

Pattern

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

Name

olimpbets.kz

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': '2 months ago', 'timestamp': 1703172317, 'iso': '2023-12-21T10:25:17-05:00'} - **IPQS: Domain:** olimpbets.kz - **IPQS: IP Address:** 194.39.65.21

Pattern Type

stix

Pattern

[domain-name:value = 'olimpbets.kz']

Name

notify-service.biz

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1700136179, 'iso': '2023-11-16T07:02:59-05:00'} - **IPQS: Domain:** notify-service.biz - **IPQS: IP Address:** 185.62.58.107

Pattern Type

stix

Pattern

[domain-name:value = 'notify-service.biz']

Name

nospam.kz

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': '2 months ago', 'timestamp': 1703172316, 'iso': '2023-12-21T10:25:16-05:00'} - **IPQS: Domain:** nospam.kz - **IPQS: IP Address:** 194.39.65.21

Pattern Type

stix

Pattern

[domain-name:value = 'nospam.kz']

Name

myfawry.net

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': '3 months ago', 'timestamp': 1702544473, 'iso': '2023-12-14T04:01:13-05:00'} - **IPQS: Domain:** myfawry.net - **IPQS: IP Address:** 2.58.15.58

Pattern Type

stix

Pattern

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

Name

mundodenoticias.online

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1700041417, 'iso': '2023-11-15T04:43:37-05:00'} - **IPQS: Domain:** mundodenoticias.online - **IPQS: IP Address:** 185.196.9.76

Pattern Type

stix

Pattern

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

Name

mmegi.co

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago',

'timestamp': 1700353211, 'iso': '2023-11-18T19:20:11-05:00'} - **IPQS: Domain:** mmegi.co - **IPQS: IP Address:** 45.129.0.125

Pattern Type

stix

Pattern

[domain-name:value = 'mmegi.co']

Name

mb-ph.net

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1701858679, 'iso': '2023-12-06T05:31:19-05:00'} - **IPQS: Domain:** mb-ph.net - **IPQS: IP Address:** 193.42.36.106

Pattern Type

stix

Pattern

[domain-name:value = 'mb-ph.net']

Name

magnum-kz.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1702043410, 'iso': '2023-12-08T08:50:10-05:00'} - **IPQS: Domain:** magnum-kz.com - **IPQS: IP Address:** 45.86.163.93

Pattern Type

stix

Pattern

[domain-name:value = 'magnum-kz.com']

Name

lusofonia-mundo.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': '3 months ago', 'timestamp': 1702565114, 'iso': '2023-12-14T09:45:14-05:00'} - **IPQS: Domain:** lusofonia-mundo.com - **IPQS: IP Address:** 169.239.129.63

Pattern Type

stix

Pattern

[domain-name:value = 'lusofonia-mundo.com']

Name

ladiesclubhouse.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** Sports - **Domain Age:** {'human': '3 months ago', 'timestamp': 1702565084, 'iso': '2023-12-14T09:44:44-05:00'} - **IPQS: Domain:** ladiesclubhouse.com - **IPQS: IP Address:** 169.239.129.48

Pattern Type

stix

Pattern

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

Name

krisha-kz.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1699537901, 'iso': '2023-11-09T08:51:41-05:00'} - **IPQS: Domain:** krisha-kz.com - **IPQS: IP Address:** 35.186.223.180

Pattern Type

stix

Pattern

[domain-name:value = 'krisha-kz.com']

Name

kroal.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1702020981, 'iso': '2023-12-08T02:36:21-05:00'} - **IPQS: Domain:** kroal.com - **IPQS: IP Address:** 91.241.93.165

Pattern Type

stix

Pattern

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

Name

kejoranews.net

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1701856357, 'iso': '2023-12-06T04:52:37-05:00'} - **IPQS: Domain:** kejoranews.net - **IPQS: IP Address:** 185.158.248.85

Pattern Type

stix

Pattern

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

Name

highclub.life

Description

- **Unsafe:** False - **Server:** Caddy - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1699608158, 'iso': '2023-11-10T04:22:38-05:00'} - **IPQS: Domain:** highclub.life - **IPQS: IP Address:** 46.249.49.230

Pattern Type

stix

Pattern

[domain-name:value = 'highclub.life']

Name

get-location.net

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago',

'timestamp': 1701959176, 'iso': '2023-12-07T09:26:16-05:00'} - **IPQS: Domain:** get-location.net - **IPQS: IP Address:** 46.246.97.245

Pattern Type

stix

Pattern

[domain-name:value = 'get-location.net']

Name

get-location.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': '3 months ago', 'timestamp': 1701688515, 'iso': '2023-12-04T06:15:15-05:00'} - **IPQS: Domain:** get-location.com - **IPQS: IP Address:** 192.46.237.163

Pattern Type

stix

Pattern

[domain-name:value = 'get-location.com']

Name

fr-monde.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': '3 months ago', 'timestamp': 1702565053, 'iso': '2023-12-14T09:44:13-05:00'} - **IPQS: Domain:** fr-monde.com - **IPQS: IP Address:** 169.239.129.76

Pattern Type

stix

Pattern

[domain-name:value = 'fr-monde.com']

Name

fastnews.biz

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1700069669, 'iso': '2023-11-15T12:34:29-05:00'} - **IPQS: Domain:** fastnews.biz - **IPQS: IP Address:** 101.99.75.197

Pattern Type

stix

Pattern

[domain-name:value = 'fastnews.biz']

Name

eventnews.live

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1701678947, 'iso': '2023-12-04T03:35:47-05:00'} - **IPQS: Domain:** eventnews.live - **IPQS: IP Address:** 185.219.221.30

Pattern Type

stix

Pattern

[domain-name:value = 'eventnews.live']

Name

escortbabesluxo.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:** Computers & Internet - **Domain Age:** {'human': '4 months ago', 'timestamp': 1698673685, 'iso': '2023-10-30T09:48:05-04:00'} - **IPQS: Domain:** nonton.southernheatinggroup.com - **IPQS: IP Address:** 172.67.184.210

Pattern Type

stix

Pattern

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

Name

e-kgd.kz

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': '3 months ago', 'timestamp': 1702390890, 'iso': '2023-12-12T09:21:30-05:00'} - **IPQS: Domain:** e-kgd.kz - **IPQS: IP Address:** 194.39.65.21

Pattern Type

stix

Pattern

[domain-name:value = 'e-kgd.kz']

Name

copy-note.net

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1701176483, 'iso': '2023-11-28T08:01:23-05:00'} - **IPQS: Domain:** copy-note.net - **IPQS: IP Address:** 185.66.140.112

Pattern Type

stix

Pattern

[domain-name:value = 'copy-note.net']

Name

coazoa.com

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': '4 months ago', 'timestamp': 1698682340, 'iso': '2023-10-30T12:12:20-04:00'} - **IPQS: Domain:** coazoa.com - **IPQS: IP Address:** 169.255.59.98

Pattern Type

stix

Pattern

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

Name

clazc.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** True - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago',

'timestamp': 1700642660, 'iso': '2023-11-22T03:44:20-05:00'} - **IPQS: Domain:** clazc.com - **IPQS: IP Address:** 85.239.34.174

Pattern Type

stix

Pattern

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

Name

centent-management.net

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': '3 months ago', 'timestamp': 1700467746, 'iso': '2023-11-20T03:09:06-05:00'} - **IPQS: Domain:** centent-management.net - **IPQS: IP Address:** 193.29.59.171

Pattern Type

stix

Pattern

[domain-name:value = 'centent-management.net']

Name

cabinet-salyk.kz

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 122158 - **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': 1702390952, 'iso': '2023-12-12T09:22:32-05:00'} - **IPQS: Domain:** cabinet-salyk.kz - **IPQS: IP Address:** 194.39.65.21

Pattern Type

stix

Pattern

[domain-name:value = 'cabinet-salyk.kz']

Name

bw-guardian.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 months ago', 'timestamp': 1700349611, 'iso': '2023-11-18T18:20:11-05:00'} - **IPQS: Domain:** bw-guardian.com - **IPQS: IP Address:** 95.141.34.222

Pattern Type

stix

Pattern

[domain-name:value = 'bw-guardian.com']

Name

buildneeds.net

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': '3 months ago', 'timestamp': 1700466887, 'iso': '2023-11-20T02:54:47-05:00'} - **IPQS: Domain:** buildneeds.net - **IPQS: IP Address:** 141.94.122.19

Pattern Type

stix

Pattern

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

Name

beroxe.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1701941807, 'iso': '2023-12-07T04:36:47-05:00'} - **IPQS: Domain:** beroxe.com - **IPQS: IP Address:** 87.121.45.45

Pattern Type

stix

Pattern

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

Name

2-gis.kz

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': '2 months ago', 'timestamp': 1703168482, 'iso': '2023-12-21T09:21:22-05:00'} - **IPQS: Domain:** 2-gis.kz - **IPQS: IP Address:** 194.39.65.21

Pattern Type

stix

Pattern

[domain-name:value = '2-gis.kz']

Name

09a.co

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1701849900, 'iso': '2023-12-06T03:05:00-05:00'} - **IPQS: Domain:** 09a.co - **IPQS: IP Address:** 5.39.221.36

Pattern Type

stix

Pattern

[domain-name:value = '09a.co']

Name

06g.co

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1701849889, 'iso': '2023-12-06T03:04:49-05:00'} - **IPQS: Domain:** 06g.co - **IPQS: IP Address:** 185.130.227.29

Pattern Type

stix

Pattern

[domain-name:value = '06g.co']

Name

02s.co

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago',

'timestamp': 1701849878, 'iso': '2023-12-06T03:04:38-05:00'} - **IPQS: Domain:** 02s.co - **IPQS: IP Address:** 185.130.227.95

Pattern Type

stix

Pattern

[domain-name:value = '02s.co']

Name

jumia-egy.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1702297741, 'iso': '2023-12-11T07:29:01-05:00'} - **IPQS: Domain:** jumia-egy.com - **IPQS: IP Address:** 79.110.52.196

Pattern Type

stix

Pattern

[domain-name:value = 'jumia-egy.com']

Name

kapital-news.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1702479872, 'iso': '2023-12-13T10:04:32-05:00'} - **IPQS: Domain:** kapital-news.com - **IPQS: IP Address:** 85.17.9.73

Pattern Type

stix

Pattern

[domain-name:value = 'kapital-news.com']

Name

ehudaldaa.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 months ago', 'timestamp': 1703244977, 'iso': '2023-12-22T06:36:17-05:00'} - **IPQS: Domain:** ehudaldaa.com - **IPQS: IP Address:** 84.247.51.14

Pattern Type

stix

Pattern

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

Name

vlast-news.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1702043011, 'iso': '2023-12-08T08:43:31-05:00'} - **IPQS: Domain:** vlast-news.com - **IPQS: IP Address:** 185.156.172.20

Pattern Type

stix

Pattern

[domain-name:value = 'vlast-news.com']

Name

ztb-news.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1702042995, 'iso': '2023-12-08T08:43:15-05:00'} - **IPQS: Domain:** ztb-news.com - **IPQS: IP Address:** 185.156.172.17

Pattern Type

stix

Pattern

[domain-name:value = 'ztb-news.com']

Name

fast-notify.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1702033942, 'iso': '2023-12-08T06:12:22-05:00'} - **IPQS: Domain:** fast-notify.com - **IPQS: IP Address:** 79.110.52.179

Pattern Type

stix

Pattern

[domain-name:value = 'fast-notify.com']

Name

dzhabarzan.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1701948230, 'iso': '2023-12-07T06:23:50-05:00'} - **IPQS: Domain:** dzhabarzan.com - **IPQS: IP Address:** 37.120.222.115

Pattern Type

stix

Pattern

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

Name

kollesa.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1699538362, 'iso': '2023-11-09T08:59:22-05:00'} - **IPQS: Domain:** kollesa.com - **IPQS: IP Address:** 217.70.184.50

Pattern Type

stix

Pattern

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

Name

mastershop.biz

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4

months ago', 'timestamp': 1700161796, 'iso': '2023-11-16T14:09:56-05:00'} - **IPQS: Domain:** mastershop.biz - **IPQS: IP Address:** 193.42.36.84

Pattern Type

stix

Pattern

[domain-name:value = 'mastershop.biz']

Name

peticaonline.com

Description

- **Unsafe:** True - **Server:** Apache/2.4.6 (Ce - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1701006694, 'iso': '2023-11-26T08:51:34-05:00'} - **IPQS: Domain:** peticaonline.com - **IPQS: IP Address:** 164.215.103.143

Pattern Type

stix

Pattern

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

Name

plinkypong.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1701170436, 'iso': '2023-11-28T06:20:36-05:00'} - **IPQS: Domain:** plinkypong.com - **IPQS: IP Address:** 146.70.161.50

Pattern Type

stix

Pattern

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

Name

post-notify.info

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1700152014, 'iso': '2023-11-16T11:26:54-05:00'} - **IPQS: Domain:** post-notify.info - **IPQS: IP Address:** 23.137.248.95

Pattern Type

stix

Pattern

[domain-name:value = 'post-notify.info']

Name

corporatebusinesssolution.net

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1700816179, 'iso': '2023-11-24T03:56:19-05:00'} - **IPQS: Domain:** corporatebusinesssolution.net - **IPQS: IP Address:** 193.168.143.184

Pattern Type

stix

Pattern

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

Name

informationrank.net

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1700816190, 'iso': '2023-11-24T03:56:30-05:00'} - **IPQS: Domain:** informationrank.net - **IPQS: IP Address:** 193.168.143.185

Pattern Type

stix

Pattern

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

Name

msbsck.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1700135200, 'iso': '2023-11-16T06:46:40-05:00'} - **IPQS: Domain:** msbsck.com - **IPQS: IP Address:** 193.29.104.83

Pattern Type

stix

Pattern

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

Name

schedulefestival.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1700044924, 'iso': '2023-11-15T05:42:04-05:00'} - **IPQS: Domain:** schedulefestival.com - **IPQS: IP Address:** 213.252.246.152

Pattern Type

stix

Pattern

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

Name

ongsworld.com

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1700053898, 'iso': '2023-11-15T08:11:38-05:00'} - **IPQS: Domain:** ongsworld.com - **IPQS: IP Address:** 146.70.158.144

Pattern Type

stix

Pattern

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

Name

gabzmus.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago',

'timestamp': 1699958804, 'iso': '2023-11-14T05:46:44-05:00'} - **IPQS: Domain:** gabzmus.com - **IPQS: IP Address:** 193.29.104.13

Pattern Type

stix

Pattern

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

Name

mujmbosnoticias.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1698673650, 'iso': '2023-10-30T09:47:30-04:00'} - **IPQS: Domain:** mujmbosnoticias.com - **IPQS: IP Address:** 185.212.47.75

Pattern Type

stix

Pattern

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

Name

nur-news.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1702479885, 'iso': '2023-12-13T10:04:45-05:00'} - **IPQS: Domain:** nur-news.com - **IPQS: IP Address:** 85.17.9.74

Pattern Type

stix

Pattern

[domain-name:value = 'nur-news.com']

Name

vinho-online.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1702565153, 'iso': '2023-12-14T09:45:53-05:00'} - **IPQS: Domain:** vinho-online.com - **IPQS: IP Address:** 169.239.128.137

Pattern Type

stix

Pattern

[domain-name:value = 'vinho-online.com']

Name

astanapark.com

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1702042933, 'iso': '2023-12-08T08:42:13-05:00'} - **IPQS: Domain:** astanapark.com - **IPQS: IP Address:** 87.121.45.42

Pattern Type

stix

Pattern

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

Malware

Name
Predator

Intrusion-Set

Name
Predator

Attack-Pattern

Name
T1583.003
ID
T1583.003
Description
Adversaries may rent Virtual Private Servers (VPSs) that can be used during targeting. There exist a variety of cloud service providers that will sell virtual machines/containers as a service. By utilizing a VPS, adversaries can make it difficult to physically tie back operations to them. The use of cloud infrastructure can also make it easier for adversaries to rapidly provision, modify, and shut down their infrastructure. Acquiring a VPS for use in later stages of the adversary lifecycle, such as Command and Control, can allow adversaries to benefit from the ubiquity and trust associated with higher reputation cloud service providers. Adversaries may also acquire infrastructure from VPS service providers that are known for renting VPSs with minimal registration information, allowing for more anonymous acquisitions of infrastructure.(Citation: TrendmicroHideoutsLease)
Name
Exploitation for Client Execution
ID
T1203

Description

Adversaries may exploit software vulnerabilities in client applications to execute code. Vulnerabilities can exist in software due to unsecure coding practices that can lead to unanticipated behavior. Adversaries can take advantage of certain vulnerabilities through targeted exploitation for the purpose of arbitrary code execution. Oftentimes the most valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility. Several types exist: ### Browser-based Exploitation Web browsers are a common target through [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) and [Spearphishing Link](https://attack.mitre.org/techniques/T1566/002). Endpoint systems may be compromised through normal web browsing or from certain users being targeted by links in spearphishing emails to adversary controlled sites used to exploit the web browser. These often do not require an action by the user for the exploit to be executed. ### Office Applications Common office and productivity applications such as Microsoft Office are also targeted through [Phishing](https://attack.mitre.org/techniques/T1566). Malicious files will be transmitted directly as attachments or through links to download them. These require the user to open the document or file for the exploit to run. ### Common Third-party Applications Other applications that are commonly seen or are part of the software deployed in a target network may also be used for exploitation. Applications such as Adobe Reader and Flash, which are common in enterprise environments, have been routinely targeted by adversaries attempting to gain access to systems. Depending on the software and nature of the vulnerability, some may be exploited in the browser or require the user to open a file. For instance, some Flash exploits have been delivered as objects within Microsoft Office documents.

Name

T1583.004

ID

T1583.004

Description

Adversaries may buy, lease, or rent physical servers that can be used during targeting. Use of servers allows an adversary to stage, launch, and execute an operation. During post-

compromise activity, adversaries may utilize servers for various tasks, including for Command and Control. Adversaries may use web servers to support support watering hole operations, as in [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), or email servers to support [Phishing](https://attack.mitre.org/techniques/T1566) operations. Instead of compromising a third-party [Server](https://attack.mitre.org/techniques/T1584/004) or renting a [Virtual Private Server](https://attack.mitre.org/techniques/T1583/003), adversaries may opt to configure and run their own servers in support of operations. Adversaries may only need a lightweight setup if most of their activities will take place using online infrastructure. Or, they may need to build extensive infrastructure if they want to test, communicate, and control other aspects of their activities on their own systems.(Citation: NYTStuxnet)

Name

T1583.001

ID

T1583.001

Description

Adversaries may acquire domains that can be used during targeting. Domain names are the human readable names used to represent one or more IP addresses. They can be purchased or, in some cases, acquired for free. Adversaries may use acquired domains for a variety of purposes, including for [Phishing](https://attack.mitre.org/techniques/T1566), [Drive-by Compromise](https://attack.mitre.org/techniques/T1189), and Command and Control.(Citation: CISA MSS Sep 2020) Adversaries may choose domains that are similar to legitimate domains, including through use of homoglyphs or use of a different top-level domain (TLD).(Citation: FireEye APT28)(Citation: PaypalScam) Typosquatting may be used to aid in delivery of payloads via [Drive-by Compromise](https://attack.mitre.org/techniques/T1189). Adversaries may also use internationalized domain names (IDNs) and different character sets (e.g. Cyrillic, Greek, etc.) to execute "IDN homograph attacks," creating visually similar lookalike domains used to deliver malware to victim machines.(Citation: CISA IDN ST05-016)(Citation: tt_httrack_fake_domains)(Citation: tt_obliqueRAT)(Citation: httrack_unhcr)(Citation: lazgroup_idn_phishing) Adversaries may also acquire and repurpose expired domains, which may be potentially already allowlisted/trusted by defenders based on an existing reputation/history.(Citation: Categorisation_not_boundary) (Citation: Domain_Steal_CC)(Citation: Redirectors_Domain_Fronting)(Citation: bypass_webproxy_filtering) Domain registrars each maintain a publicly viewable database that displays contact information for every registered domain. Private WHOIS services

display alternative information, such as their own company data, rather than the owner of the domain. Adversaries may use such private WHOIS services to obscure information about who owns a purchased domain. Adversaries may further interrupt efforts to track their infrastructure by using varied registration information and purchasing domains with different domain registrars.(Citation: Mandiant APT1)

Name

T1566.002

ID

T1566.002

Description

Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearphishing. It is different from other forms of spearphishing in that it employs the use of links to download malware contained in email, instead of attaching malicious files to the email itself, to avoid defenses that may inspect email attachments. Spearphishing may also involve social engineering techniques, such as posing as a trusted source. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this case, the malicious emails contain links. Generally, the links will be accompanied by social engineering text and require the user to actively click or copy and paste a URL into a browser, leveraging [User Execution](https://attack.mitre.org/techniques/T1204). The visited website may compromise the web browser using an exploit, or the user will be prompted to download applications, documents, zip files, or even executables depending on the pretext for the email in the first place. Adversaries may also include links that are intended to interact directly with an email reader, including embedded images intended to exploit the end system directly. Additionally, adversaries may use seemingly benign links that abuse special characters to mimic legitimate websites (known as an "IDN homograph attack").(Citation: CISA IDN ST05-016) URLs may also be obfuscated by taking advantage of quirks in the URL schema, such as the acceptance of integer- or hexadecimal-based hostname formats and the automatic discarding of text before an “@” symbol: for example, `hxxp://google.com@1157586937`.(Citation: Mandiant URL Obfuscation 2023) Adversaries may also utilize links to perform consent phishing, typically with OAuth 2.0 request URLs that when accepted by the user provide permissions/access for malicious applications, allowing adversaries to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s.(Citation: Trend Micro Pawn Storm OAuth 2017) These stolen access tokens allow

the adversary to perform various actions on behalf of the user via API calls. (Citation: Microsoft OAuth 2.0 Consent Phishing 2021)

Country

Name
Saudi Arabia
Name
Oman
Name
Armenia
Name
Philippines
Name
Indonesia
Name
Mongolia
Name
Kazakhstan

Name
Trinidad and Tobago
Name
Botswana
Name
Angola
Name
Egypt

Region

Name
Middle East
Name
South-eastern Asia
Name
Eastern Asia
Name
Central Asia
Name
Asia
Name
Latin America and the Caribbean
Name
Americas

Name
Sub-Saharan Africa
Name
Northern Africa
Name
Africa

Domain-Name

Value
zikolo.net
zakorn.com
yo-um7.com
weekendcool.com
walatparez.com
vestinfos.net
vestinfo.org
vestinfo.net
vendaswebs.com
ulstur.co
tohna.net
tobupmi.com
tickets-kz.com

thintank.co

sustanbuild.com

suarapapua.co

sportnow.news

spacsaver.info

soccer-bw.com

shoxtek.com

rozavetrovv.com

rcuples.com

qazsporttv.com

plastictoysworld.com

people-beeline.com

pelovkin.com

olimpbets.kz

notify-service.biz

nospam.kz

myfawry.net

mundodenoticias.online

mmegi.co

mb-ph.net

magnum-kz.com

lusofonia-mundo.com

ladiesclubhouse.com

kroal.com

krisha-kz.com

kejoranews.net

highclub.life

get-location.net

get-location.com

fr-monde.com

fastnews.biz

eventnews.live

escortbabesluxo.com

e-kgd.kz

copy-note.net

coazoa.com

clazc.com

centent-management.net

cabinet-salyk.kz

bw-guardian.com

buildneeds.net

beroxe.com

2-gis.kz

09a.co

06g.co

02s.co

jumia-egy.com

ehudaldaa.com

kapital-news.com

vlast-news.com

ztb-news.com

fast-notify.com

kollesa.com

dzhabarzan.com

mastershop.biz
peticaonline.com
post-notify.info
plinkypong.com
corporatebusinesssolution.net
informationrank.net
msbsck.com
schedulefestival.com
gabzmus.com
ongsworld.com
mujmbosnoticias.com
nur-news.com
vinho-online.com
astanapark.com

External References

- https://www.recordedfuture.com/predator-spyware-operators-rebuild-multi-tier-infrastructure-target-mobile-devices
- https://otx.alienvault.com/pulse/65e5e21fa7cd4bdf46a01aa5