Feb 22 2024

NETMANAGEIT

Intelligence Report

Operation Texonto: Information operation targeting Ukrainian speakers in the context of the war

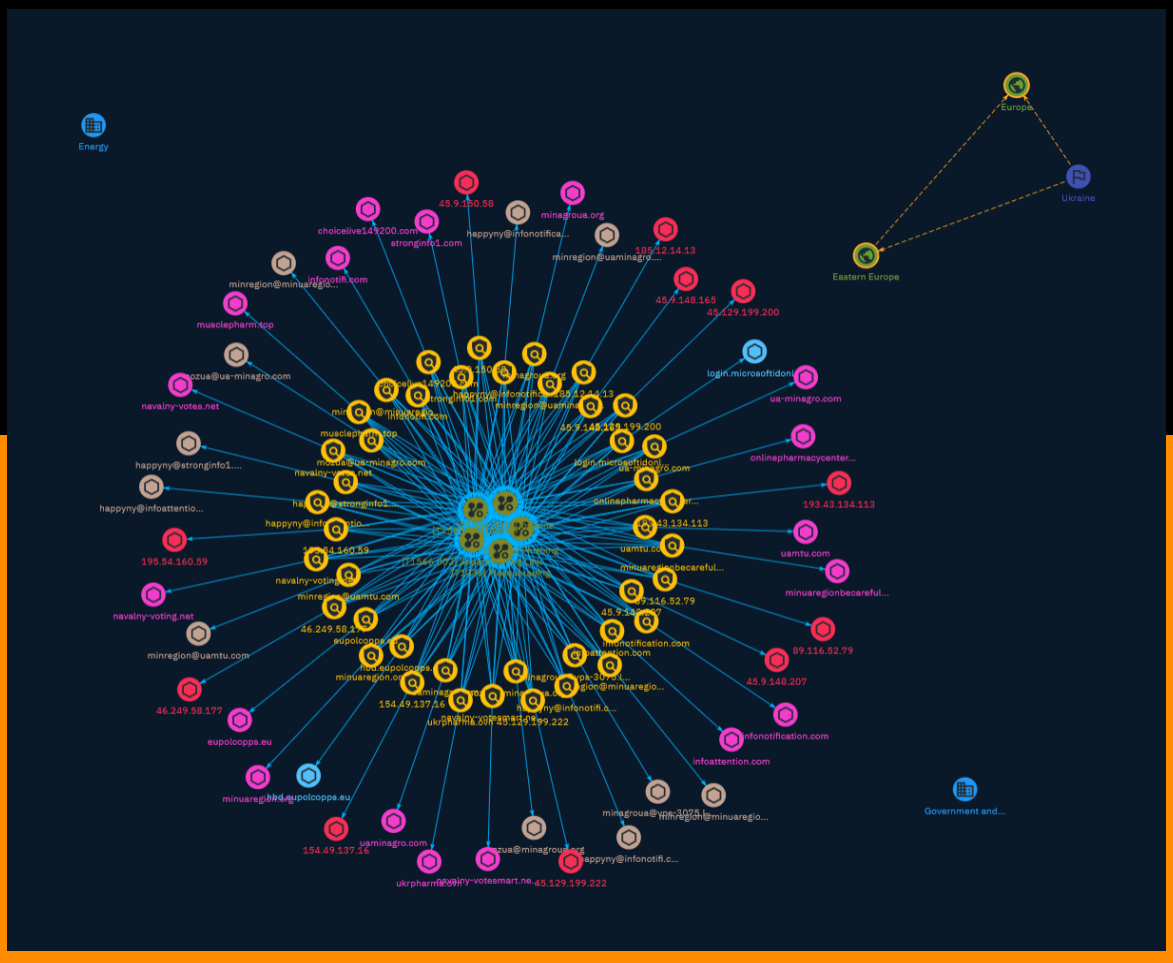

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A disinformation and psychological operation campaign called Operation Texonto used spam emails to target Ukrainian speakers. The emails contained fabricated messages about heating, medicine, and food shortages due to the war, aiming to demoralize the recipients. The campaign had two waves, one in November 2023 and another in December.

Confidence

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

15 / 100

Content

N/A

Indicator

Name
login.microsoftidonline.com
Pattern Type
stix
Pattern
[hostname:value = 'login.microsoftidonline.com']
Name
hbd.eupolcopps.eu
Pattern Type
stix
Pattern
[hostname:value = 'hbd.eupolcopps.eu']
Name
minregion@uaminagro.com

Description

- **Valid:** False - **Disposable:** False - **SMTP Score:** 0 - **Overall Score:** 0 - **First Name:** Unknown - **Generic:** False - **Common:** False - **DNS Valid:** False - **Honeypot:** False - **Deliverability:** low - **Frequent Complainer:** False - **Spam Trap Score:** none - **Catch All:** False - **Timed Out:** False - **Suspect:** False - **Recent Abuse:** False - **Suggested Domain:** N/A - **Leaked:** False - **Sanitized Email:** minregion@uaminagro.com - **Domain Age:** {'human': '3 months ago', 'timestamp': 1699963548, 'iso': '2023-11-14T07:05:48-05:00'} - **First Seen:** {'human': '7 hours ago', 'timestamp': 1708570638, 'iso': '2024-02-21T21:57:18-05:00'}

Pattern Type

stix

Pattern

[email-addr:value = 'minregion@uaminagro.com']

Name

mozua@ua-minagro.com

Description

- **Valid:** False - **Disposable:** False - **SMTP Score:** 0 - **Overall Score:** 0 - **First Name:** Unknown - **Generic:** False - **Common:** False - **DNS Valid:** False - **Honeypot:** False - **Deliverability:** low - **Frequent Complainer:** False - **Spam Trap Score:** none - **Catch All:** False - **Timed Out:** False - **Suspect:** False - **Recent Abuse:** False - **Suggested Domain:** N/A - **Leaked:** False - **Sanitized Email:** mozua@ua-minagro.com - **Domain Age:** {'human': '3 months ago', 'timestamp': 1699963552, 'iso': '2023-11-14T07:05:52-05:00'} - **First Seen:** {'human': '7 hours ago', 'timestamp': 1708570649, 'iso': '2024-02-21T21:57:29-05:00'}

Pattern Type

stix

Pattern

[email-addr:value = 'mozua@ua-minagro.com']

Name

minregion@uamtu.com

Description

- **Valid:** False - **Disposable:** False - **SMTP Score:** 0 - **Overall Score:** 0 - **First Name:** Unknown - **Generic:** False - **Common:** False - **DNS Valid:** False - **Honeypot:** False - **Deliverability:** low - **Frequent Complainer:** False - **Spam Trap Score:** none - **Catch All:** False - **Timed Out:** False - **Suspect:** False - **Recent Abuse:** False - **Suggested Domain:** N/A - **Leaked:** False - **Sanitized Email:** minregion@uamtu.com - **Domain Age:** {'human': '3 months ago', 'timestamp': 1699970664, 'iso': '2023-11-14T09:04:24-05:00'} - **First Seen:** {'human': '7 hours ago', 'timestamp': 1708570649, 'iso': '2024-02-21T21:57:29-05:00'}

Pattern Type

stix

Pattern

[email-addr:value = 'minregion@uamtu.com']

Name

minregion@minuaregionbecareful.com

Description

- **Valid:** False - **Disposable:** False - **SMTP Score:** 0 - **Overall Score:** 0 - **First Name:** Unknown - **Generic:** False - **Common:** False - **DNS Valid:** False - **Honeypot:** False - **Deliverability:** low - **Frequent Complainer:** False - **Spam Trap Score:** none - **Catch All:** False - **Timed Out:** False - **Suspect:** False -

Recent Abuse: False - **Suggested Domain:** N/A - **Leaked:** False - **Sanitized Email:** minregion@minuaregionbecareful.com - **Domain Age:** {'human': '3 months ago', 'timestamp': 1700221417, 'iso': '2023-11-17T06:43:37-05:00'} - **First Seen:** {'human': '7 hours ago', 'timestamp': 1708570645, 'iso': '2024-02-21T21:57:25-05:00'}

Pattern Type

stix

Pattern

[email-addr:value = 'minregion@minuaregionbecareful.com']

Name

mozua@minagroua.org

Description

- **Valid:** False - **Disposable:** False - **SMTP Score:** 0 - **Overall Score:** 0 - **First Name:** Unknown - **Generic:** False - **Common:** False - **DNS Valid:** False - **Honeypot:** False - **Deliverability:** low - **Frequent Complainer:** False - **Spam Trap Score:** none - **Catch All:** False - **Timed Out:** False - **Suspect:** False - **Recent Abuse:** False - **Suggested Domain:** N/A - **Leaked:** False - **Sanitized Email:** mozua@minagroua.org - **Domain Age:** {'human': '3 months ago', 'timestamp': 1699963548, 'iso': '2023-11-14T07:05:48-05:00'} - **First Seen:** {'human': '7 hours ago', 'timestamp': 1708570650, 'iso': '2024-02-21T21:57:30-05:00'}

Pattern Type

stix

Pattern

[email-addr:value = 'mozua@minagroua.org']

Name

minregion@minuaregion.org

Description

- **Valid:** True - **Disposable:** False - **SMTP Score:** 2 - **Overall Score:** 3 - **First Name:** Unknown - **Generic:** False - **Common:** False - **DNS Valid:** True - **Honeypot:** False - **Deliverability:** medium - **Frequent Complainer:** False - **Spam Trap Score:** none - **Catch All:** True - **Timed Out:** False - **Suspect:** True - **Recent Abuse:** False - **Suggested Domain:** N/A - **Leaked:** False - **Sanitized Email:** minregion@minuaregion.org - **Domain Age:** {'human': '3 months ago', 'timestamp': 1699970660, 'iso': '2023-11-14T09:04:20-05:00'} - **First Seen:** {'human': '7 hours ago', 'timestamp': 1708570645, 'iso': '2024-02-21T21:57:25-05:00'}

Pattern Type

stix

Pattern

[email-addr:value = 'minregion@minuaregion.org']

Name

minagroua@vps-3075.lethost.network

Description

- **Valid:** False - **Disposable:** False - **SMTP Score:** 0 - **Overall Score:** 0 - **First Name:** Unknown - **Generic:** False - **Common:** False - **DNS Valid:** False - **Honeypot:** False - **Deliverability:** low - **Frequent Complainer:** False - **Spam Trap Score:** none - **Catch All:** False - **Timed Out:** False - **Suspect:** False - **Recent Abuse:** False - **Suggested Domain:** N/A - **Leaked:** False - **Sanitized Email:** minagroua@vps-3075.lethost.network - **Domain Age:** {'human': '2 years ago', 'timestamp': 1654645026, 'iso': '2022-06-07T19:37:06-04:00'} - **First Seen:** {'human': '7 hours ago', 'timestamp': 1708570651, 'iso': '2024-02-21T21:57:31-05:00'}

Pattern Type

stix

Pattern

[email-addr:value = 'minagroua@vps-3075.lethost.network']

Name

happyny@infonotification.com

Description

- **Valid:** True - **Disposable:** False - **SMTP Score:** 1 - **Overall Score:** 2 - **First Name:** Happy - **Generic:** False - **Common:** False - **DNS Valid:** True - **Honeypot:** False - **Deliverability:** low - **Frequent Complainer:** False - **Spam Trap Score:** none - **Catch All:** False - **Timed Out:** False - **Suspect:** True - **Recent Abuse:** False - **Suggested Domain:** N/A - **Leaked:** False - **Sanitized Email:** happyny@infonotification.com - **Domain Age:** {'human': '4 months ago', 'timestamp': 1698322693, 'iso': '2023-10-26T08:18:13-04:00'} - **First Seen:** {'human': '7 hours ago', 'timestamp': 1708570663, 'iso': '2024-02-21T21:57:43-05:00'}

Pattern Type

stix

Pattern

[email-addr:value = 'happyny@infonotification.com']

Name

happyny@stronginfo1.com

Description

- **Valid:** True - **Disposable:** False - **SMTP Score:** 2 - **Overall Score:** 3 - **First Name:** Happy - **Generic:** False - **Common:** False - **DNS Valid:** True -

Honeypot: False - **Deliverability:** medium - **Frequent Complainer:** False - **Spam Trap Score:** none - **Catch All:** True - **Timed Out:** False - **Suspect:** True - **Recent Abuse:** False - **Suggested Domain:** N/A - **Leaked:** False - **Sanitized Email:** happyny@stronginfo1.com - **Domain Age:** {'human': '4 months ago', 'timestamp': 1698322688, 'iso': '2023-10-26T08:18:08-04:00'} - **First Seen:** {'human': '7 hours ago', 'timestamp': 1708570653, 'iso': '2024-02-21T21:57:33-05:00'}

Pattern Type

stix

Pattern

[email-addr:value = 'happyny@stronginfo1.com']

Name

happyny@infonotifi.com

Description

- **Valid:** True - **Disposable:** False - **SMTP Score:** 1 - **Overall Score:** 2 - **First Name:** Happy - **Generic:** False - **Common:** False - **DNS Valid:** True - **Honeypot:** False - **Deliverability:** low - **Frequent Complainer:** False - **Spam Trap Score:** none - **Catch All:** False - **Timed Out:** False - **Suspect:** True - **Recent Abuse:** False - **Suggested Domain:** N/A - **Leaked:** False - **Sanitized Email:** happyny@infonotifi.com - **Domain Age:** {'human': '4 months ago', 'timestamp': 1698322693, 'iso': '2023-10-26T08:18:13-04:00'} - **First Seen:** {'human': '2 months ago', 'timestamp': 1703822791, 'iso': '2023-12-28T23:06:31-05:00'}

Pattern Type

stix

Pattern

[email-addr:value = 'happyny@infonotifi.com']

Name

happyny@infoattention.com

Description

- **Valid:** False - **Disposable:** False - **SMTP Score:** 0 - **Overall Score:** 0 - **First Name:** Unknown - **Generic:** False - **Common:** False - **DNS Valid:** False - **Honeypot:** False - **Deliverability:** low - **Frequent Complainer:** False - **Spam Trap Score:** none - **Catch All:** False - **Timed Out:** False - **Suspect:** False - **Recent Abuse:** False - **Suggested Domain:** N/A - **Leaked:** False - **Sanitized Email:** happyny@infoattention.com - **Domain Age:** {'human': '4 months ago', 'timestamp': 1698322683, 'iso': '2023-10-26T08:18:03-04:00'} - **First Seen:** {'human': '7 hours ago', 'timestamp': 1708570652, 'iso': '2024-02-21T21:57:32-05:00'}

Pattern Type

stix

Pattern

[email-addr:value = 'happyny@infoattention.com']

Name

uamtu.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '3 months ago', 'timestamp': 1699970664, 'iso': '2023-11-14T09:04:24-05:00'} - **IPQS: Domain:** uamtu.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

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

Name

uaminagro.com

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 months ago', 'timestamp': 1699963548, 'iso': '2023-11-14T07:05:48-05:00'} - **IPQS: Domain:** uaminagro.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

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

Name

ua-minagro.com

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 months ago',

'timestamp': 1699963552, 'iso': '2023-11-14T07:05:52-05:00'} - **IPQS: Domain:** ua-minagro.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'ua-minagro.com']

Name

stronginfo1.com

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1698322688, 'iso': '2023-10-26T08:18:08-04:00'} - **IPQS: Domain:** stronginfo1.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[domain-name:value = 'stronginfo1.com']

Name

navalny-voting.net

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '5 months ago', 'timestamp': 1694263304, 'iso': '2023-09-09T08:41:44-04:00'} - **IPQS: Domain:** navalny-voting.net - **IPQS: IP Address:** 104.21.46.50

Pattern Type

stix

Pattern

[domain-name:value = 'navalny-voting.net']

Name

onlinepharmacycenter.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': '8 months ago', 'timestamp': 1686903357, 'iso': '2023-06-16T04:15:57-04:00'} - **IPQS: Domain:** onlinepharmacycenter.com - **IPQS: IP Address:** 45.227.252.239

Pattern Type

stix

Pattern

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

Name

navalny-votesmart.net

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '5 months ago', 'timestamp': 1694263308, 'iso': '2023-09-09T08:41:48-04:00'} - **IPQS: Domain:** navalny-votesmart.net - **IPQS: IP Address:** 172.67.133.44

Pattern Type

stix

Pattern

[domain-name:value = 'navalny-votesmart.net']

Name

navalny-votes.net

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '5 months ago', 'timestamp': 1694263304, 'iso': '2023-09-09T08:41:44-04:00'} - **IPQS: Domain:** navalny-votes.net - **IPQS: IP Address:** 104.21.38.150

Pattern Type

stix

Pattern

[domain-name:value = 'navalny-votes.net']

Name

minuaregionbecareful.com

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 months ago', 'timestamp': 1700221417, 'iso': '2023-11-17T06:43:37-05:00'} - **IPQS: Domain:** minuaregionbecareful.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

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

Name

minuaregion.org

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 months ago', 'timestamp': 1699970660, 'iso': '2023-11-14T09:04:20-05:00'} - **IPQS: Domain:** minuaregion.org - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

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

Name

minagroua.org

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 months ago', 'timestamp': 1699963548, 'iso': '2023-11-14T07:05:48-05:00'} - **IPQS: Domain:** minagroua.org - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

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

Name

infonotification.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': 1698322693, 'iso': '2023-10-26T08:18:13-04:00'} - **IPQS: Domain:** infonotification.com - **IPQS: IP Address:** 185.12.14.13

Pattern Type

stix

Pattern

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

Name

eupolcopps.eu

Description

- **Unsafe:** False - **Server:** Apache - **Domain Rank:** 226412 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** Political organizations - **Domain Age:** {'human': '2 years ago', 'timestamp': 1636764407, 'iso': '2021-11-12T19:46:47-05:00'} - **IPQS: Domain:** eupolcopps.eu - **IPQS: IP Address:** 5.104.228.229

Pattern Type

stix

Pattern

[domain-name:value = 'eupolcopps.eu']

Name

infonotifi.com

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': 1698322693, 'iso': '2023-10-26T08:18:13-04:00'} - **IPQS: Domain:** infonotifi.com - **IPQS: IP Address:** 46.249.58.177

Pattern Type

stix

Pattern

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

Name

infoattention.com

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': '4 months ago', 'timestamp': 1698322683, 'iso': '2023-10-26T08:18:03-04:00'} - **IPQS: Domain:** infoattention.com - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

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

Name

choicelive149200.com

Description

- **Unsafe:** False - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** False - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '4 months ago', 'timestamp': 1698322683, 'iso': '2023-10-26T08:18:03-04:00'} - **IPQS: Domain:** choicelive149200.com - **IPQS: IP Address:** 104.21.12.15

Pattern Type

stix

Pattern

[domain-name:value = 'choicelive149200.com']

Name

89.116.52.79

Description

- **Zip Code:** N/A - **ISP:** Hostinger International - **ASN:** 47583 - **Organization:** Hostinger International - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** 89.116.52.79 - **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:** Drenthe - **City:** Meppel - **Latitude:** 52.7 - **Longitude:** 6.18

Pattern Type

stix

Pattern

[ipv4-addr:value = '89.116.52.79']

Name

46.249.58.177

Description

- **Zip Code:** N/A - **ISP:** Serverius Holding - **ASN:** 50673 - **Organization:** Serverius Holding - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** infonotifi.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:** Utrecht - **City:** Nieuwegein - **Latitude:** 52.03 - **Longitude:** 5.09

Pattern Type

stix

Pattern

[ipv4-addr:value = '46.249.58.177']

Name

45.9.148.165

Description

- **Zip Code:** N/A - **ISP:** Nice IT Services Group - **ASN:** 49447 - **Organization:** Nice IT Services Group - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** infoattention.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:** North Holland - **City:** Amsterdam - **Latitude:** 52.37 - **Longitude:** 4.89

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.9.148.165']

Name

45.129.199.222

Description

- **Zip Code:** N/A - **ISP:** BlueVPS OU - **ASN:** 62005 - **Organization:** BlueVPS OU - **Is Crawler:** False - **Timezone:** Europe/Tallinn - **Mobile:** False - **Host:** mta0.wearethecarguy.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:** EE - **Region:** Harjumaa - **City:** Tallinn - **Latitude:** 59.44 - **Longitude:** 24.74

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.129.199.222']

Name

185.12.14.13

Description

- **Zip Code:** N/A - **ISP:** Serverius Holding - **ASN:** 50673 - **Organization:** Serverius Holding - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** infonotification.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:** North Brabant - **City:** Eindhoven - **Latitude:** 51.44 - **Longitude:** 5.48

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.12.14.13']

Name

45.129.199.200

Description

- **Zip Code:** N/A - **ISP:** BlueVPS OU - **ASN:** 62005 - **Organization:** BlueVPS OU - **Is Crawler:** False - **Timezone:** Europe/Tallinn - **Mobile:** False - **Host:** minuaregion.org - **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:** EE - **Region:** Harjumaa - **City:** Tallinn - **Latitude:** 59.44 - **Longitude:** 24.74

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.129.199.200']

Name

154.49.137.16

Description

- **Zip Code:** N/A - **ISP:** Cogent Communications - **ASN:** 47583 - **Organization:** Hostinger International - **Is Crawler:** False - **Timezone:** Europe/Paris - **Mobile:** False - **Host:** 154.49.137.16 - **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:** FR - **Region:** le-de-France - **City:** La Courneuve - **Latitude:** 48.92 - **Longitude:** 2.4

Pattern Type

stix

Pattern

[ipv4-addr:value = '154.49.137.16']

Name

45.9.150.58

Description

- **Zip Code:** N/A - **ISP:** Nice IT Services Group - **ASN:** 49447 - **Organization:** Nice IT Services Group - **Is Crawler:** False - **Timezone:** Europe/Zurich - **Mobile:** False - **Host:** stronginfo1.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:** CH - **Region:** Bern - **City:** Bern - **Latitude:** 46.95 - **Longitude:** 7.45

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.9.150.58']

Name

45.9.148.207

Description

- **Zip Code:** N/A - **ISP:** Nice IT Services Group - **ASN:** 49447 - **Organization:** Nice IT Services Group - **Is Crawler:** False - **Timezone:** Europe/Amsterdam - **Mobile:** False - **Host:** 45.9.148.207 - **Proxy:** True - **VPN:** False - **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:** North Holland - **City:** Amsterdam - **Latitude:** 52.3716011 - **Longitude:** 4.88829994

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.9.148.207']

Name

195.54.160.59

Description

- **Zip Code:** N/A - **ISP:** BlueVPS OU - **ASN:** 62005 - **Organization:** BlueVPS OU - **Is Crawler:** False - **Timezone:** Europe/Rome - **Mobile:** False - **Host:** minagroua.org - **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:** IT - **Region:** Sicily - **City:** Palermo - **Latitude:** 38.13 - **Longitude:** 13.33

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.54.160.59']

Name

193.43.134.113

Description

- **Zip Code:** N/A - **ISP:** Hostinger International - **ASN:** 47583 - **Organization:** Hostinger International - **Is Crawler:** False - **Timezone:** America/Phoenix - **Mobile:** False - **Host:** 193.43.134.113 - **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:** US - **Region:** Arizona - **City:** Phoenix - **Latitude:** 33.45 - **Longitude:** -112.09

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.43.134.113']

Name
ukrpharma.ovh
Pattern Type
stix
Pattern
[domain-name:value = 'ukrpharma.ovh']
Name
musclepharm.top
Pattern Type
stix
Pattern
[domain-name:value = 'musclepharm.top']

Attack-Pattern

Name
Phishing
ID
T1566
Description
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Server

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

Domains

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

Masquerading

ID

T1036

Description

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

T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

Spearphishing Link

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
Ukraine

Region

Name
Eastern Europe

Name
Europe

Sector

Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.
Name
Energy
Description
Public and private entities operating to extract, store, transport and process fuel, entities managing energy plants and energy storage and distribution and entities managing fuel waste.

Hostname

Value
login.microsoftidonline.com
hbd.eupolcopps.eu

Email-Addr

Value
mozua@ua-minagro.com
mozua@minagroua.org
minregion@uamtu.com
minregion@uaminagro.com
minregion@minuaregionbecareful.com
minregion@minuaregion.org
minagroua@vps-3075.lethost.network
happyny@stronginfo1.com
happyny@infonotification.com
happyny@infonotifi.com
happyny@infoattention.com

Domain-Name

Value
uamtu.com
uaminagro.com
stronginfo1.com
ua-minagro.com
navalny-voting.net
onlinepharmacycenter.com
navalny-votesmart.net
navalny-votes.net
minuaregionbecareful.com
minuaregion.org
minagroua.org
infonotification.com
infonotifi.com

infoattention.com
eupolcopps.eu
choicelive149200.com
ukrpharma.ovh
musclepharm.top

IPv4-Addr

Value
89.116.52.79
46.249.58.177
45.9.148.165
45.129.199.222
45.129.199.200
185.12.14.13
154.49.137.16
45.9.150.58
45.9.148.207
195.54.160.59
193.43.134.113

External References

- https://www.welivesecurity.com/en/eset-research/operation-texonto-information-operation-targeting-ukrainian-speakers-context-war/
- https://otx.alienvault.com/pulse/65d714481708e0f9a359b8c8