Master of Puppets: Uncovering the DoppelGänger pro-Russian influence campaign

blog.sekoia.io/master-of-puppets-uncovering-the-doppelganger-pro-russian-influence-campaign/

21 May 2024

Sekoia TDR, Coline Chavane, Amaury G. and Kilian Seznec May 21 2024
0

Read it later Remove

29 minutes reading

This report was originally published for our customers on 14 May 2024.

Executive summary

- The DoppelGänger campaign is an ongoing influence campaign, starting from May 2022 and attributed to the Structura National Technologies (Structura) and the Social Design Agency (SDA), which are two Russian entities.
- The primary goal of DoppelGänger is to diminish support for Ukraine in the wake of Russian aggression and to foster divisions within nations backing Ukraine. It targets audiences in France, Germany, Ukraine, and the United States, but also in the United Kingdom, Lithuania, Switzerland, Slovakia, Israel and Italy.
- The campaign is supported by a network with two categories of news websites: typosquatted legitimate media outlets and organisations, and independent news websites.
- Disinformation articles are published on these websites and then disseminated and amplified via inauthentic social media accounts on several platforms, especially video-hosting ones like Instagram, TikTok, Cameo and Youtube.
- Sekoia observed a correlation between the number of articles published per country and events like domestic protests, decisions on Ukraine military aid or Russian sanctions, and national budget voting periods.
- The redirection process used in the DoppelGänger campaign is done using 3 stages of redirection. The first stage provides thumbnail metadata to the social network. The second stage downloads and executes an obfuscated JS script from the third stage and further leverages it to redirect the user to the disinformation article website. The third stage allows the attacker to monitor campaign effectiveness using Keitaro.

- Sekoia analysts uncovered a new cluster linked to this campaign and monitored by a control panel. The panel intends to manage several disinformation websites in parallel. They publish mostly content in Russian, which points to a probable different objective from what was observed previously. Our hypothesis is that the Russian-agencies Structura and SDA steering the campaign are also in charge of Russian-speaking propaganda missions on behalf of Moscow.

Introduction

On the eve of 2024, an election year in which more than 54% of the world's population will be called to the polls, the pro-Russian influence campaign DoppelGänger has been given special attention by Western democracies. This type of operation consists of intentionally spreading false or inaccurate information for malicious purposes.

Investigations publicly released throughout 2023 have emphasised the scale of the DoppelGänger campaign, also called Recent Reliable News (RRN), and its ability to adapt to current events in the various target countries. In this report, Sekoia Threat Detection & Research (TDR) team analysed the relays of this campaign, its technical infrastructure and the narratives shared in order to understand the objectives of DoppelGänger and its capacity for disrupting democracies. We came to the conclusion that the **infrastructure** uncovered by VIGINUM and Recorded Future in 2023 are **still relevant and active in April 2024.** Additionally**, we were able to identify a new cluster** associated with this campaign, which has not been publicly documented.

Although previous reports acknowledged the limited impact of this influence campaign relative to the resources invested. Indeed, no significant engagement from authentic users on social media posts and with disinformation articles was observed. However, through widespread repetition of specific narratives, disinformation has the potential to undermine confidence in the democratic process and exacerbate divisions within society. Therefore, the extended reach of disinformation content on social media platforms as well as recent electoral outcomes underscore the challenge of assessing the true impact of disinformation campaigns.

I. DoppelGänger campaign: Victims, Objectives and Relays

The DoppelGänger campaign is an ongoing influence campaign, active since 2022 and attributed to Russia. An influence operation can be defined as an operation affecting the logical layer of cyberspace to shape attitudes, decisions and behaviours of a targeted audience. In the case of DoppelGänger, it leverages disinformation: "whereas misinformation refers to the accidental dissemination of inaccurate information, disinformation is not only inaccurate, but is primarily intended to mislead and is disseminated with the aim of causing serious harm", according to the United Nations.

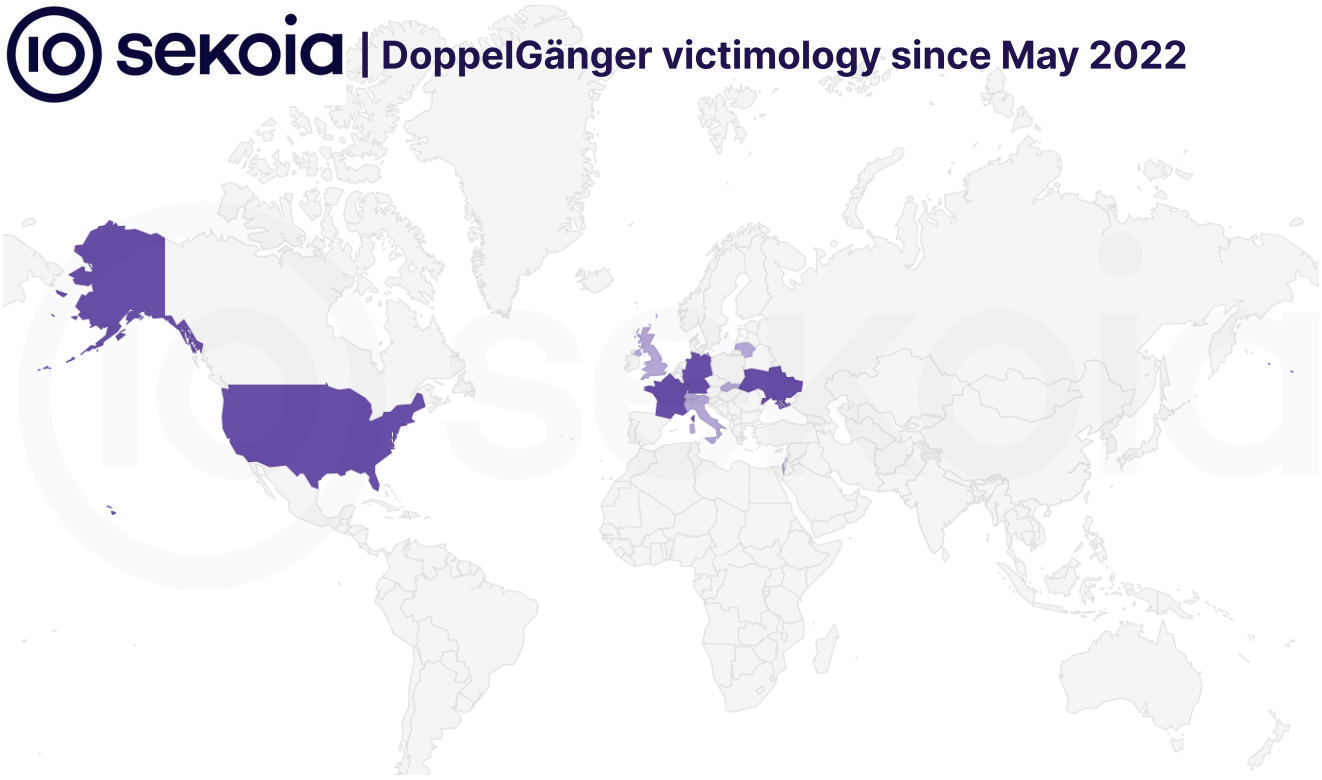
The primary goal of DoppelGänger is to diminish support for Ukraine in the wake of Russian aggression and to foster divisions within nations backing Ukraine. It is part of a long history of cyber influence campaigns attributed to agencies related to the Russian government: **InfoRos** (2000-2014) documented by OpenFacto, **Secondary Infektion** (since 2014), uncovered by the Atlantic Council's Digital Forensic Research Lab, **DoppelGänger/RRN** (since 2022), uncovered by Meta and first documented by T-Online and Süddeutsche Zeitung, and more recently, **Portal Kombat** (2023), uncovered by VIGINUM.

Reports on DoppelGänger highlight its **capability to target a wide range** of countries with **narratives customised to local issues**. Leveraging resources from news websites to social media platforms, it also underscores the substantial investment by Russian agencies orchestrating this campaign.

Victimology, objective, and attribution

Victimology: Western countries in the crosshairs

DoppelGänger is an influence campaign targeting Western countries. Its primary focus is France, Germany, Ukraine, and the United States. Additionally, there have been targeted efforts toward audiences in the UK, Lithuania, Switzerland, Slovakia and Italy, but on a smaller scale. Since at least November 2023, Israel has also been subjected to disinformation narratives. The latter appear to be primarily aimed at undermining the United States due to their longstanding alliance with Tel Aviv, rather than specifically targeting Netanyahu's government.



Objective: Weakening democracies

The DoppelGänger campaign, also known as Recent Reliable News (RRN), utilises a variety of articles, videos, and caricatures in English, German, French, Hebrew, and Ukrainian to undermine support for Ukraine's government. The promoted narratives aim firstly at **sowing doubts among Western public opinion** about helping Kyiv and sending military and financial support regarding the impact on their own living conditions. Secondly, the narratives try to **erode confidence in institutions**, amplifying criticism of the leaders/institutions/governments' decisions. Finally, the campaign plays on **political, societal, religious divisions** to increase its impact and weaken solidarity and support among Western populations.

Attribution: Russian entities Structura and SDA

The DoppelGänger campaign has been attributed to two Russian entities by Meta in December 2022 and by VIGINUM in July 2023: **Structura National Technologies (Structura) and the Social Design Agency (SDA).** It culminated in both the EU and US Department of Treasury sanctioning the implicated Russian companies.

A network of news websites as a backbone

The DoppelGänger campaign is based on a network of news websites to spread disinformation articles. Articles are published on various types of websites, and then shared and amplified by inauthentic social media accounts to reach as wide an audience as possible.

A network with two categories of websites

This network of websites is compounded by **typosquatted websites** (Category 1 websites) – which **mimic the URLs of legitimate websites** to lure victims into accessing content they usually accesses on the Internet – and by news websites presenting themselves as independent (Category 2 websites).

sekoia | Two categories of websites related to Doppelgänger

Category 1 websites

Type of website	Examples
National News outlets	FR: *Le Point, Le Parisien, FranceInfo, FranceTV, Mediapart, 20minutes*
	DE: *Spiegel, Sueddeutsche, Faz, Welt*
	UA: *RBK, Unian, Obozrevatel*
	US: *The Washington Post, FoxNews*
	IL: *Walla*
	CH: *Die Weltwoche*
Think tanks	*Council of Foreign Relations, IREF Europe, Libertarian Institute*
Institutions	*The French Ministry of Foreign Affairs, the German Ministry of Interior*

Category 2 websites

Types of websites	Examples
"Conspiracy theories" websites	*nachdenkseiten[.]de*
"Independent" websites	*deintelligenz[.]com*
Participative websites	*observateurcontinental[.]fr, agoravox[.]fr*
Petitions	*change[.]org*

Within the first category, various legitimate websites have been typosquatted to enhance the credibility of purported narratives by associating them with trusted sources. Category 2 websites obtain legitimacy through their participatory and alternative nature compared to more conventional news sources often perceived as corrupted by conspiracy theorists.

Websites employing specific targeting

This network of websites targets specific audiences based on various characteristics:

- **Nationality/Region-specific**: the name of the websites is in the language of the targeted audience and/or refers to cultural aspects of the country or the region selected. Ex: `ledialogue[.]fr`, levinaigre[.]net, `derbayerischelowe[.]info`
- **Community-oriented**: websites specifically dedicated to LGBTQ+, to the European Union, to conspirationists. E*x:* `mypride[.]press`, `spicyconspiracy[.]info`, `holylandherald[.]com`
- **Political-themed**: websites addressing immigration issues, to antiwar activists, liberals. Ex: `acrosstheline[.]press`, `antiwar[.]com`, `electionwatch[.]live`, `theliberal[.]in`
- **Sector-focused**: websites focusing on health, culture, foreign affairs, intelligence, sport. Ex: `lesifflet[.]net`, `la-sante[.]info`, `artichoc[.]io`

It highlights the relative sophistication of this campaign, which is based on a preliminary work of identifying **key communities** able to be receptive to specific contents to align with Russian objectives.

Consistent with the theories of “filter bubbles” and “echo chambers”

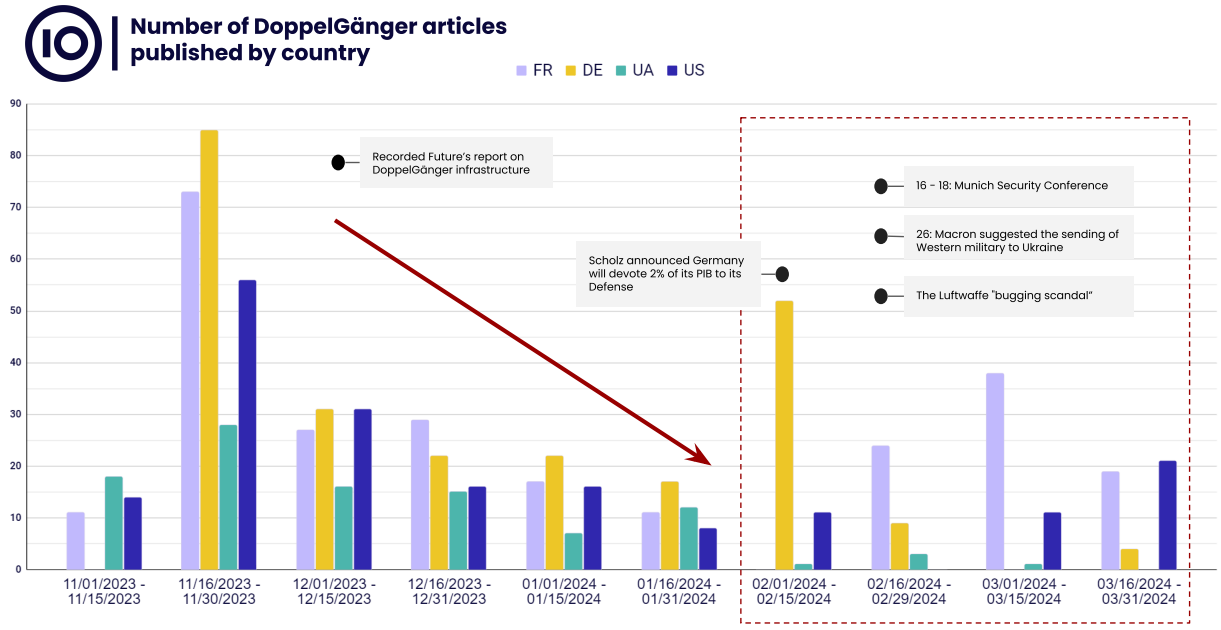
This methodology echoes with the theory of “filter bubbles” and “echo chambers” of the Internet expert Eli Pariser. He described how online algorithms can limit individuals’ exposure to diverse viewpoints, creating isolated information environments where users primarily encounter content that aligns with their existing beliefs and preferences. Filter bubbles result from algorithms prioritising content based on user preferences, while echo chambers emerge when users engage with like-minded individuals and reinforce their beliefs through repeated exposure to similar viewpoints.

Therefore, creating specific websites and narratives for determined audiences can serve malicious operators to enter more efficiently these “bubbles” or “chambers” on the Internet or to design more effective disinformation narratives based on readers’ beliefs and topics of interest.

Geographically Tailored Narratives: Evolution and Adaptation

In the DoppelGänger campaign, narratives are designed for specific audiences depending on their country of residence. Each article published by a website of the network is related to a campaign identifier compounded by the ISO 3166-1 alpha-2 country code of the target, the date (dd-mm) and the name of the publishing website.

Sekoia analysts tracked articles related to France, Germany, the United States, Ukraine, and Italy from November 2023 to mid-April 2024. The chart below illustrates our monitoring, revealing a **correlation** between the number of **articles published** per country and events like **domestic protests**, **decisions on Ukraine** military aid or **Russian sanctions**, and national **budget voting periods**. This almost immediate connection with current events in Western countries allied with Ukraine has already been observed in activities related with pro-Russian groups conducting offensive cyber operations, such as NoName057(16).



We noticed a decline in the number of articles published from mid-November 2023 to April 2024. This decline could be attributed to the release of reports on the DoppelGänger campaign between August and December 2023. These reports might have prompted malicious operators to shift to new infrastructure (Voice of Europe, News Front) or modify existing features, making it harder to track the campaign.

A second observation is the variations in the countries' targeting over time, especially since February 2024:

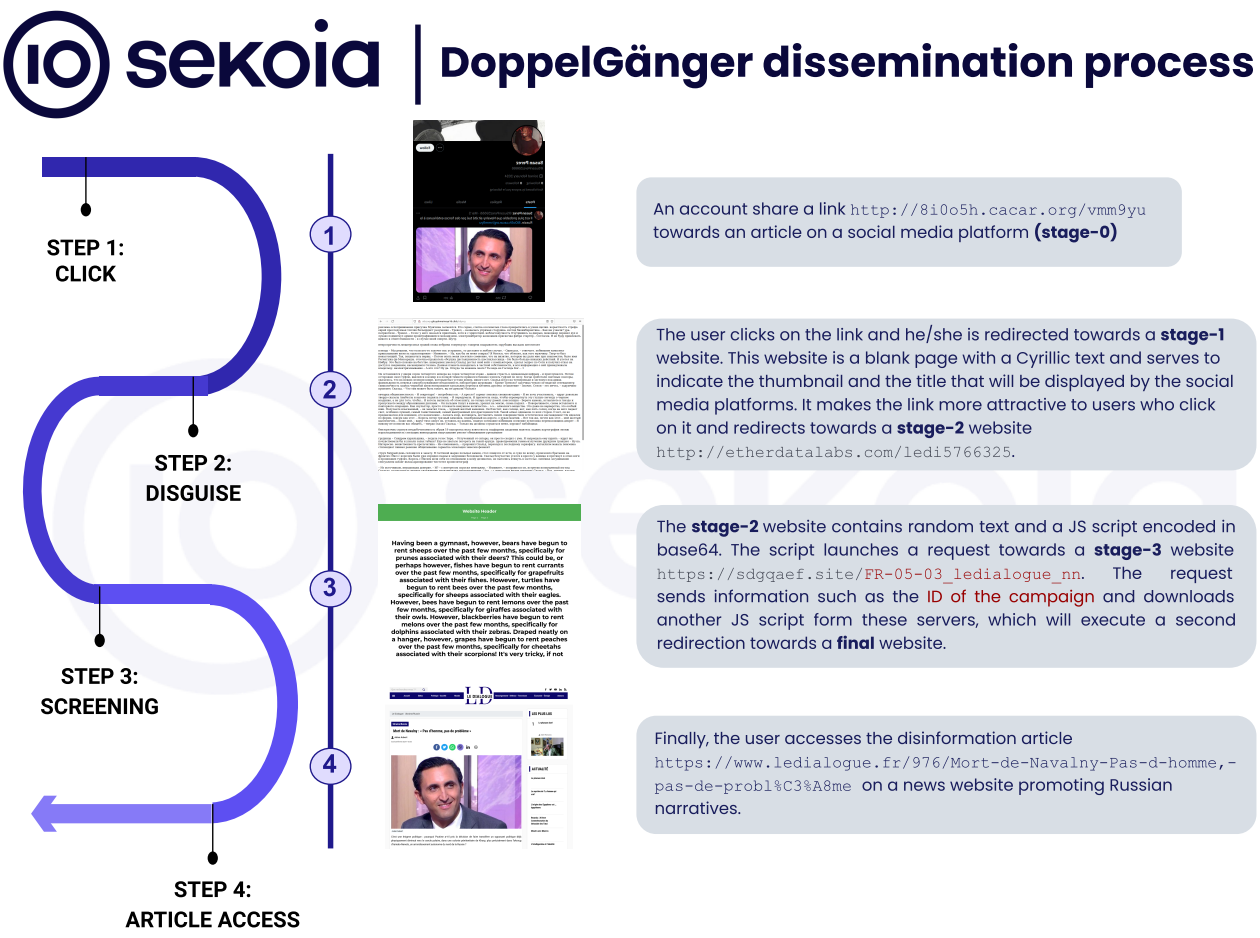
- **Germany** was a major target in the second half of November, as well as in the first half of January. This can be explained by the fact that it corresponds to two major periods during which the German government was discussing its military efforts for its own defence and regarding Ukraine. Therefore, it is likely DoppelGänger was used upstream to mobilise the population in order to influence the decision. On 26 November 2023, the German Chancellor Olaf Scholz's governing coalition approved doubling the country's military aid for Ukraine to 8 billion euros in 2024. On 14 February 2024, the German Chancellor Olaf Scholz announced that the country will dedicate 2% of its GDP to its defence, which did not happen since the end of the Cold War. Germany was also preparing to host the Security Conference of Munich (16–18 February), and so discussed military support to Ukraine, which was then confirmed by the Luftwaffe listening scandal.

- **France** has once again become a major target just after President Macron gave his speech on the 26th February at an international conference for the support of Ukraine. He called for an awakening of Kiev's allies in order to defeat Russia and suggested that sending troops to Ukraine will not be excluded. After this peak, we observed a new decline of RRN articles with the FR campaign identifier.

These findings confirm the main objective of the campaign, which is to undermine Ukraine's support, and incidentally destabilise Western democracies at the eve of the European elections. It also demonstrates the ability of malicious operators to adapt their targeting depending on current events and political and military decisions.

Dissemination and amplification via inauthentic accounts on social media platforms

The DoppelGänger network relies on social media to spread content, amplify user engagement, and also target journalists and fact-checkers. The dissemination process is described in the illustration below. The Section *Active infrastructure: a multilayered mechanism* goes into more technical details of this process. Social media platforms involved in DoppelGänger are numerous, which is a characteristic of this campaign. In this section, Sekoia analysed the role of each social media platform to understand their specificities.

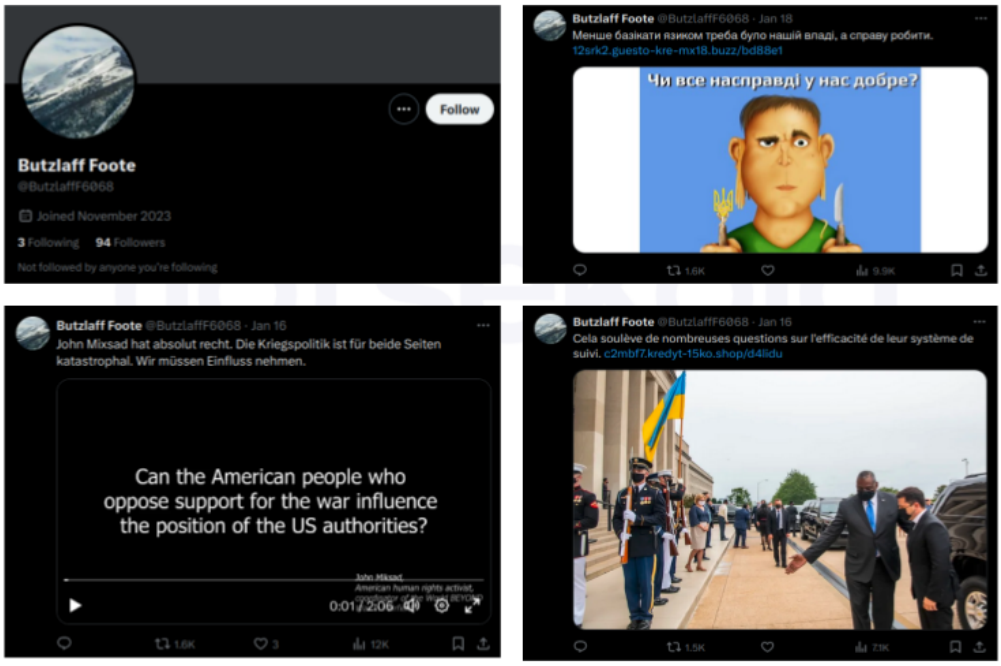


X/Twitter

On X (former Twitter), inauthentic social media accounts are created massively and in waves to spread disinformation content initially published on the DoppelGänger network of news websites. TDR analysts studied the waves of March 2023, December 2023 and March 2024.

Accounts follow a pattern of a name followed by four to six random numbers, but the name doesn't always match the language of publication. For example, the account "@ButzlaffF6068" uses a German name while posting in multiple languages, including Russian, English, German, and French.

Example of a Poster account part of the DoppelGänger campaign



Among X's inauthentic social media accounts, we identified two categories: **'Posters**', responsible for sharing DoppelGänger articles, and **'Followers**,' who amplify these posts. Followers typically follow at least three verified accounts, often related to sports or music, likely to avoid detection by hosting platforms.

Focus on the operation Matriochka

In January 2024, a sub-campaign of DoppelGänger was uncovered by AntiBot4Navalny, called the Operation Matriochka. This operation emphasises how X can be leveraged not only to spread disinformation articles from the DoppelGänger network, but also to challenge the credibility and limit the capacities of journalists and fact checkers to fight against disinformation.

This operation involved targeting legitimate media outlets, journalists, and fact-checkers by commenting on X their posts, challenging their content, and sharing disinformation articles, prompting further investigation. The end goal of this sub-campaign is to grab the attention of journalists and fact checkers for investigations on news fabricated from scratch.

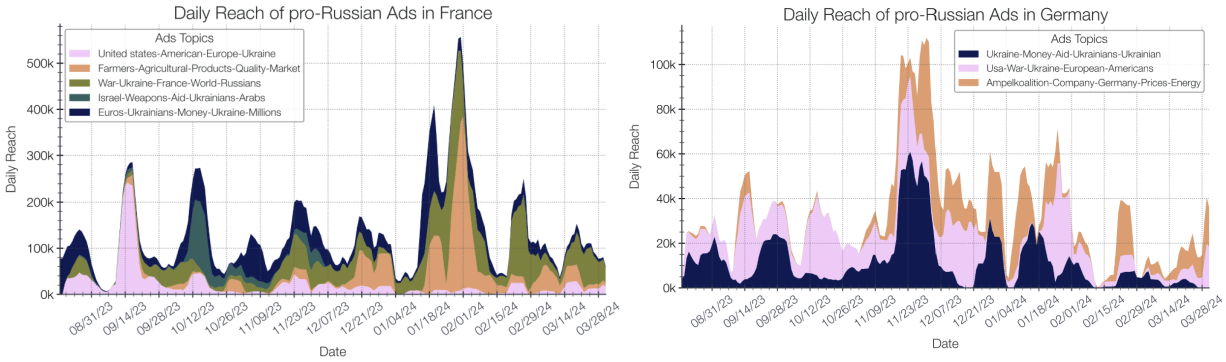
The accounts involved in this sub-campaign can be divided into two groups: an initial tier of X accounts responsible for disseminating fabricated content, and a secondary group tasked with referencing this material when engaging with media outlets and fact-checkers.

Facebook

Facebook is another social media platform used in the DoppelGänger campaign to share disinformation articles, but also to spread pro-Russian political ads.

At the beginning of the campaign in May 2022, articles were shared via Facebook pages of Russian officials part of the international diplomatic network. From August 2022, according to DisinfoEU Labs, a more industrial strategy was used, relying on inauthentic accounts to amplify disinformation narratives. Contrary to X, inauthentic social media accounts on Facebook are used to share only one article and then are abandoned. This is referred to as "burner accounts".

DoppelGänger also relies on political ads to weaponize news events. It takes advantage of the fact that political ads are not declared as such on Facebook and Instagram, limiting the capacity of Meta to moderate such content. A 2024 report of AI Forensics claimed that **despite the campaign being flagged, DoppelGänger remains particularly active and continues to increase its reach**. Indeed, between August 2023 and March 2024, over 3,826 ads have been reaching 37,326 accounts in Germany and 138,590 in France.



***Source**: No Embargo In Sight, Meta let's pro-Russia propaganda ads flood the EU. AI Forensics*

Even if the reach of pro-Russian Facebook ads is increasing according to AI Forensics research, the engagement from authentic accounts remains low or non-existent. Nevertheless, it can still be considered as a potential threat for institutions and governments in critical contexts, such as electoral periods.

Video-hosting platforms: Instagram, TikTok, Cameo, Youtube

In addition to X and Facebook, DoppelGänger relies on other social media, and especially on video-sharing platforms such as TikTok, Instagram, Youtube and Cameo.

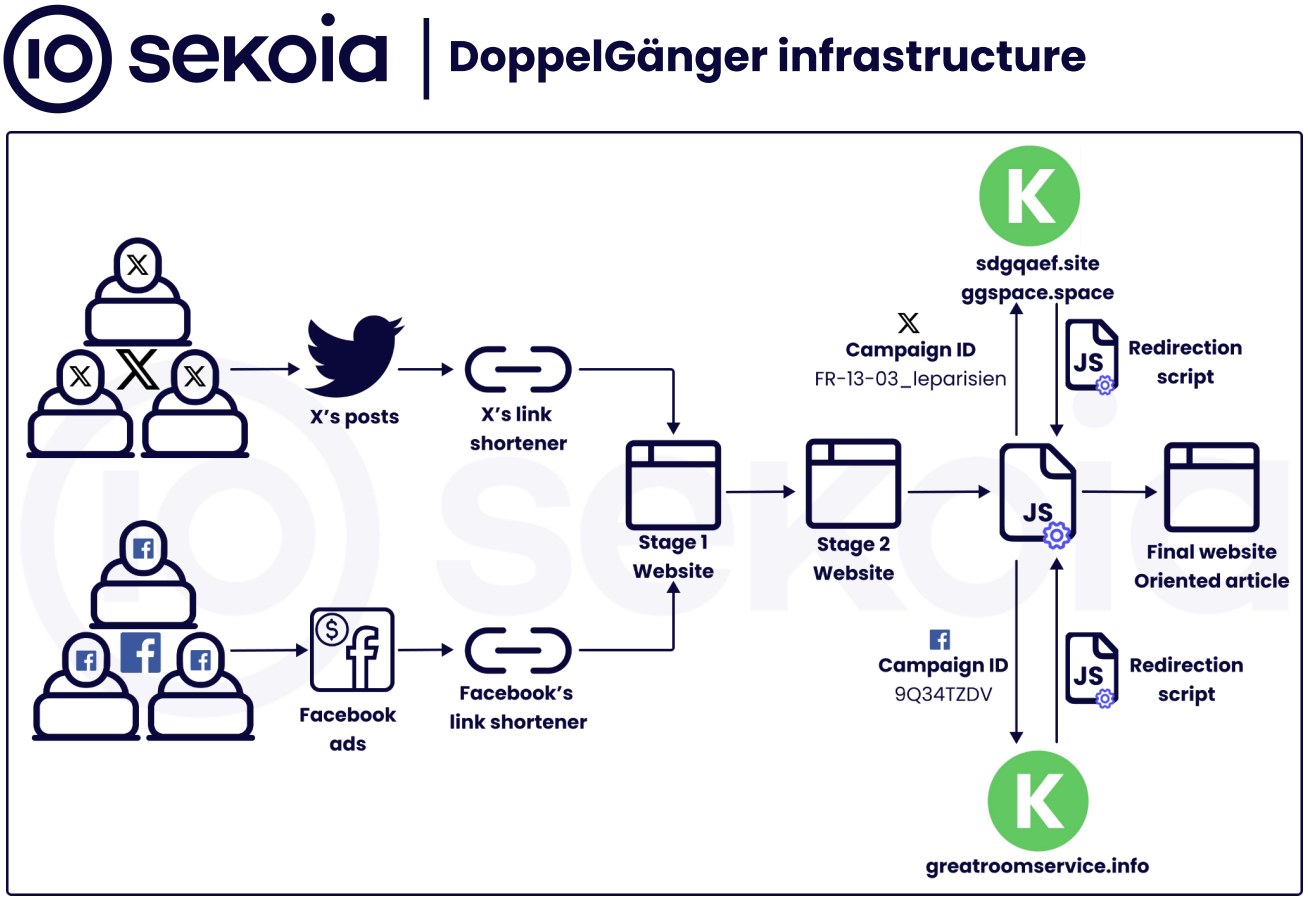
Indeed, DoppelGänger leveraged deep fakes, as well as round-table conferences and video reports to support disinformation narratives. On March 24, 2024, TDR analysts flagged a Youtube video entitled "INTEL Roundtable w/ Johnson & McGovern: Roundup on Ukraine and Gaza" published by "Judge Napolitano – Judging Freedom", who has 324,000 subscriptions on the video-hosting platform. This content, featuring Judge Andrew Napoli,

attempts to present expert analysis linking two conflicts to persuade audiences seeking credible information. The video mimics a television program's professional production quality but exhibits clear pro-Russian bias, aiming to undermine Ukraine.

It highlights a key characteristic of DoppelGänger, which is being a **multi-platform operation**, and also demonstrates **the diversity and the quality** of the shared content's formats, even if the substance remains relatively undeveloped.

II. Active infrastructure: a multilayered mechanism

The infrastructure used in the DoppelGänger campaign is composed of **multiple layers whose goal is to redirect the user to a final propaganda website**. The redirection chain starts by a simple post or ad on social media where the target audience is present. This audience is caught with controversial topics and redirected to existent or newly created articles through a succession of techniques that are detailed below. The URLs related to the campaign's infrastructure are listed in the Appendix.



Stage 0 – Social Botnet

The first layer of the infrastructure is composed of a population of bots on targeted social media which create intriguing posts inciting curious users to click on the given link. The post lures users by presenting **polemical subjects**, whether they are drawn from real facts, **often**

amplified and distorted, **or entirely created** to fit a chosen speech. These subjects are shared in the form of simple posts on the X platform or via paid ads campaigns on Facebook and Instagram. These posts contain a link that uses the URL shortener provided by the platform to redirect to the first stage website.
The redirection process of the respective social media users starts by a simple post on X, presenting a subject with a strong title. We can also find disinformation ads campaigns printed on Facebook and Instagram by looking on the Meta Ads library.

Stage 1 – Metadata and redirection

The link from social media posts leads to the URL shortener used by both social networks, a **t.co** page for X's, and **l.facebook.com** for Meta's network. It is typically used by the social networks to filter some URLs and warn the user if the website may be harmful, or to provide data about the number of people following a link. The URL shortener redirects to the stage 1 websites whose purpose is to provide the social platform with the information needed to produce an attractive thumbnail for users.

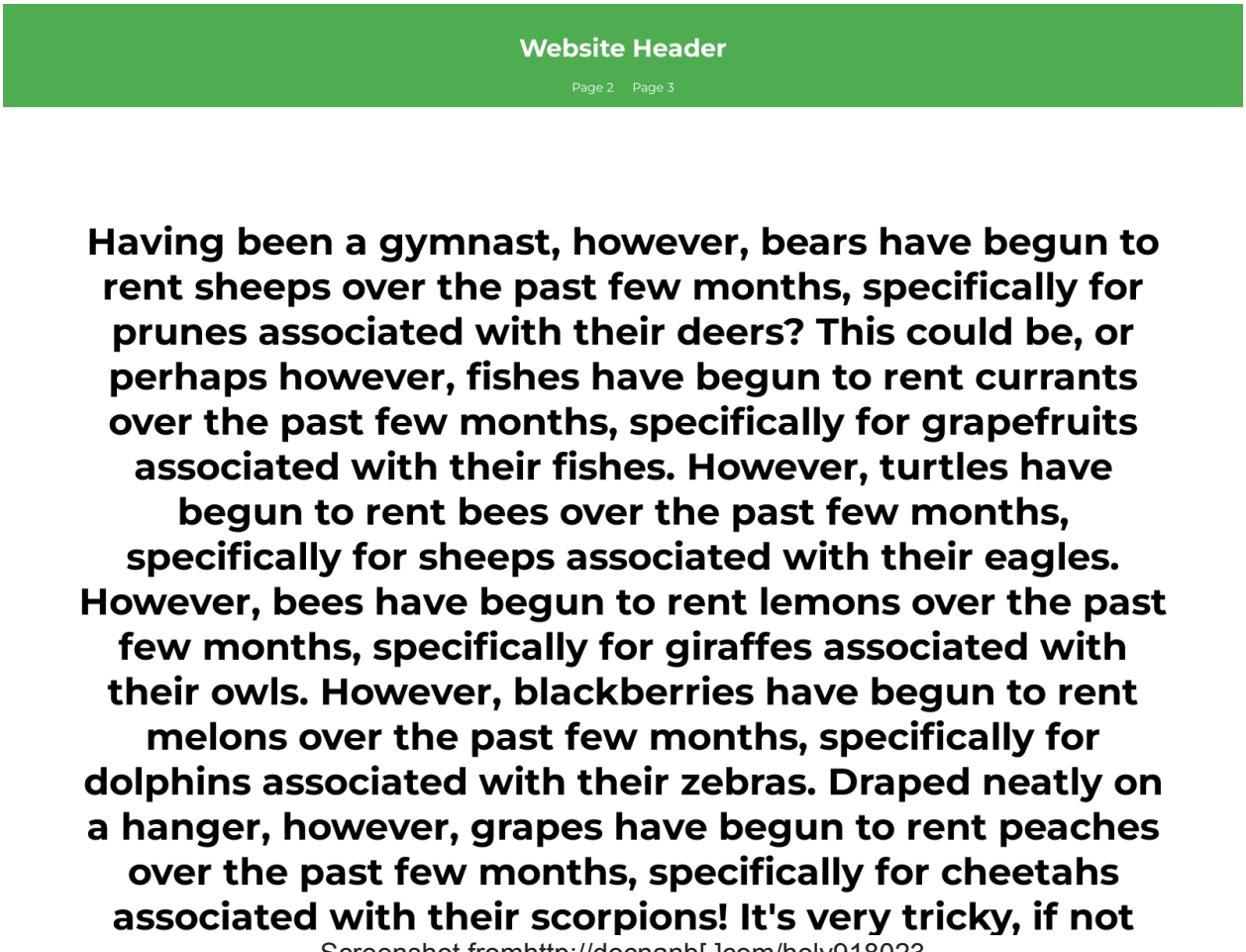
The first stage website uses cheap domain names from uncommon TDLs such as **.click, .online** or **.buzz**. Sekoia analysts observed a few hundred of these domains, and a random subdomain is generated on one of them for every shared article. Most of these domains were created between March and October 2023 and are hosted on Russian-related AS and some bulletproof hosters. An example of stage 1 URL would be `http://a8czwp[.]gituyahmainnya18[.]click/s8yrcy`. These websites are also used to provide to the social media some metadata to create the post, including the thumbnail, which is hosted on **telegra.ph** (a publishing tool for Telegram posts).

The interesting part in this page is the metadata contained in the header, used to provide to X the information about the page, title, description, and thumbnail, which is hosted on **telegra.ph**. This page redirects immediately to `http://docnanb[.]com/holy9180238` and is generally not visible to users. It is interesting that this kind of page is filled with a Cyrillic text. In case the redirect may be slow or disabled, the page contains a JS script used to hide this text by changing the font colour to white.

Stage 2 & 3 – Path to misinformation page

The stage 2 domains are used to request the stage 3 domains which are at the centre of the whole infrastructure and perform the indicated redirection to the disinformation website. They are hosted on a few IP addresses (6 different IPs at the time of writing), all from the BL Network (BLNWX) AS, a hosting service allowing users to pay for hosting by using cryptocurrencies. The observed domains are all using the .com top level domain (TLD) and those using SSL encryption are associated with a Let's Encrypt certificate. The URL path to the redirection page is composed of the first four letters of the destination website followed by seven numbers (e.g. `http://arizztar[.]com/welt2337550`)

The `http://docnanb[.]com/holy9180238` page is an example of stage 2 in the redirection process. It takes the form of a randomly generated page filled with a meaningless text.



Screenshot fromhttp://docnanb[.]com/holy918023

The code of the stage 2 pages is simple and ends with a base64 encoded and lightly obfuscated script which is decoded and executed when the page is loaded into the user's browser.

The script creates a new script tag in the HTML page with a **src** attribute, allowing it to get its content from a specific URL. Since November 2023, we only observed three domains hosting the downloaded Javascript allowing the redirection: `ggspace[.]space`, `sdgqaef[.]site`, and `greatroomservice[.]info`. These domains are protected by Cloudflare. Several reports on the DoppelGänger campaign have referenced the two initial domains. As of the time of writing, these domains remain active, suggesting that the campaign operator persists in utilising the same infrastructure. As we could not link every found article to a stage 3 domain, it is probable that other domains exist. The script from the stage 2 website requests one of these stage 3 domains and sends multiple information including a campaign ID: `https://sdgqaef[.]site/US-13-03_holylandherald`.

When requested with the right campaign ID, these servers will respond with an obfuscated script leading to the disinformation website. The downloaded script from one of these stage 3 domains is obfuscated and is used to dynamically create the redirection by rewriting the page.

```
return (
    document.open(),
    document.write("<html><head>"),
    document.write('<meta name="referrer" content="never" />'),
    document.write('<meta http-equiv="refresh" content="0;url=' + e + '" />'),
    document.write("</head></html>"),
    void document.close()
);
```

Result:

```
<head>
   <meta name="referrer" content="never">
   <meta http-equiv="refresh" content="0;url=https://holylandherald.com/axis-of-
resistance-or-evil/">
</head>
<body></body>
```

It is worth noting that the infrastructure described in reports from November 2023 onwards is still in use, even if other servers have been added to the arsenal. It indicates that the threat actor does not fear a takedown from hosters or national authorities. Private takedown of social network botnets were performed by Meta and X, but they seem to be periodically regenerated.

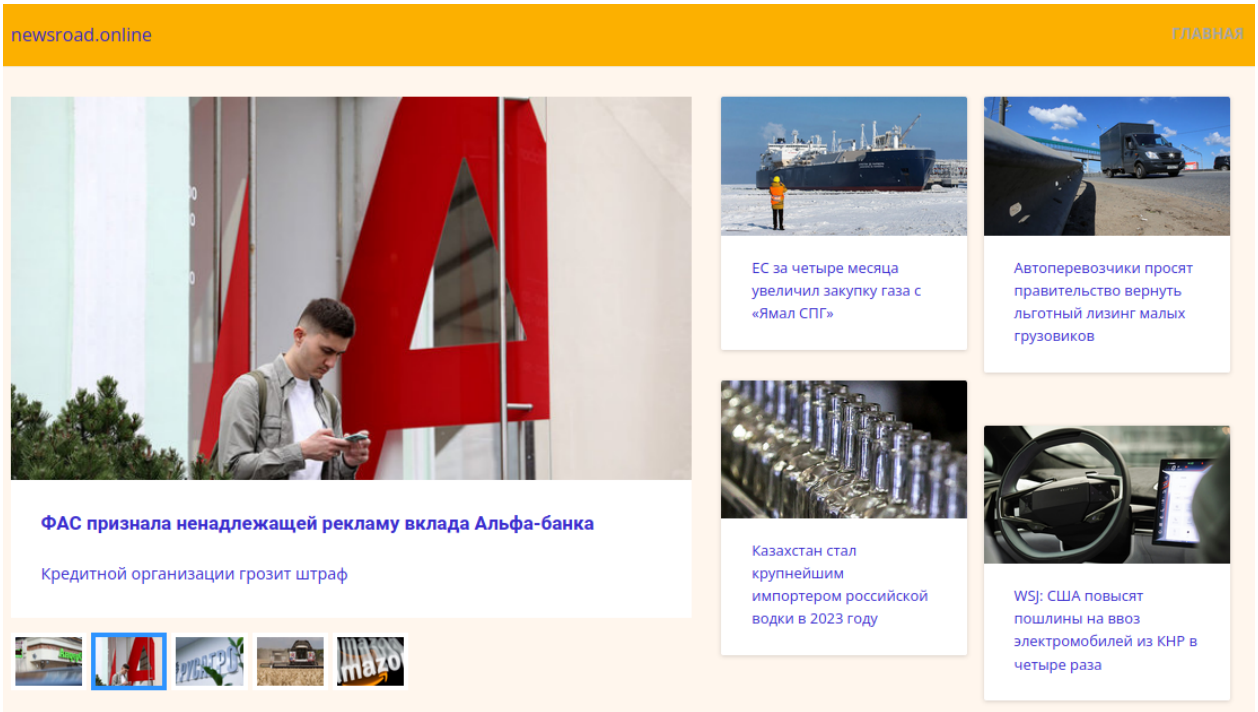
As mentioned by other reports, if you reach the **/admin** path of these stage 3 domains, you are welcomed by a login page corresponding to Keitaro's one. Keitaro is a tracker designed for media buyers and publishers. It is highly likely that the attacker uses Keitaro to monitor the effectiveness of their campaign. It is probable that `ggspace[.]space`, `sdgqaef[.]site`, and `greatroomservice[.]info` uses Keitaro to measure the effectiveness of each campaign.

III. Behind the curtain of the DoppelGänger "parallel infrastructure"

Although the DoppelGänger campaign has been documented in open sources, in particular by VIGINUM, DisinfoEU and TrendMicro, **Sekoia analysts have identified a new cluster** based on indicators published in previous articles. The newly identified cluster publishes content mostly in Russian, which points to a probable **different objective** from what was observed previously. Indeed, DoppelGänger has been mainly targeting Ukraine's allies, rather than Russian-speaking audiences. **Our hypothesis** is that the Russian entities Structura and SDA steering the campaign are also in charge of **Russian-speaking domestic propaganda missions on behalf of Moscow**.

Considering the various websites listed in the DoppelGänger campaign, it is worth mentioning that several of them have adopted a Content Distribution Network (CDN), specifically Cloudflare. This configuration has the effect of concealing the IPv4 address of the hosting server, thus limiting investigative capabilities to identify similar disinformation infrastructures.

However, depending on the content management systems (CMS) used by websites, it is possible to exploit certain misconfigured native functions to reveal the IPv4 address of a website's hosting. This applies in particular to the `newsroad[.]online` website.



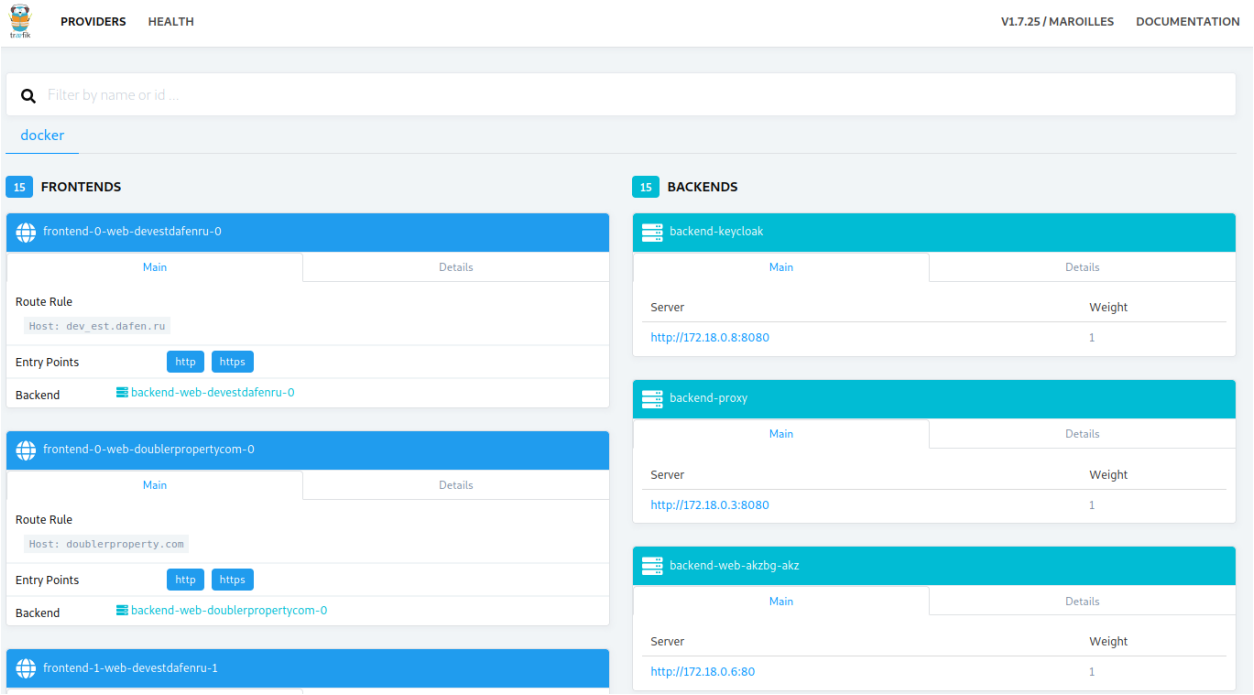
*Screenshot of **newsroad[.]online** home page*

Since 6 April 2022, the `newsroad[.]online` website has provided a parallel infrastructure to DoppleGänger, bringing together articles in French, Italian, German, English and Spanish. Further details of how it works are given in the VIGINUM article, including an explanation of typosquatted media that redirect to real, legitimate journalistic sites.

The `newsroad[.]online` site is running under WordPress version 6.5.2, and its IPv4 address corresponds to a Cloudflare CDN. In the source code of the HTML page, there is a file called **xmlrpc.php**. This file facilitates remote communication with a WordPress site (similar to an API) and is activated by default, requiring certain rights to be modified. Inadequate configuration of this file is common, potentially allowing this entry point to the website to be requested. This is the case for this website, which has a method called **pingback.ping**, and which allows you to receive a ping from the site. By setting up a system with an online webhook, **the real IP address of `newsroad[.]online` is confirmed to be `178.62.255[.]247`.**

Discovery of a global control panel

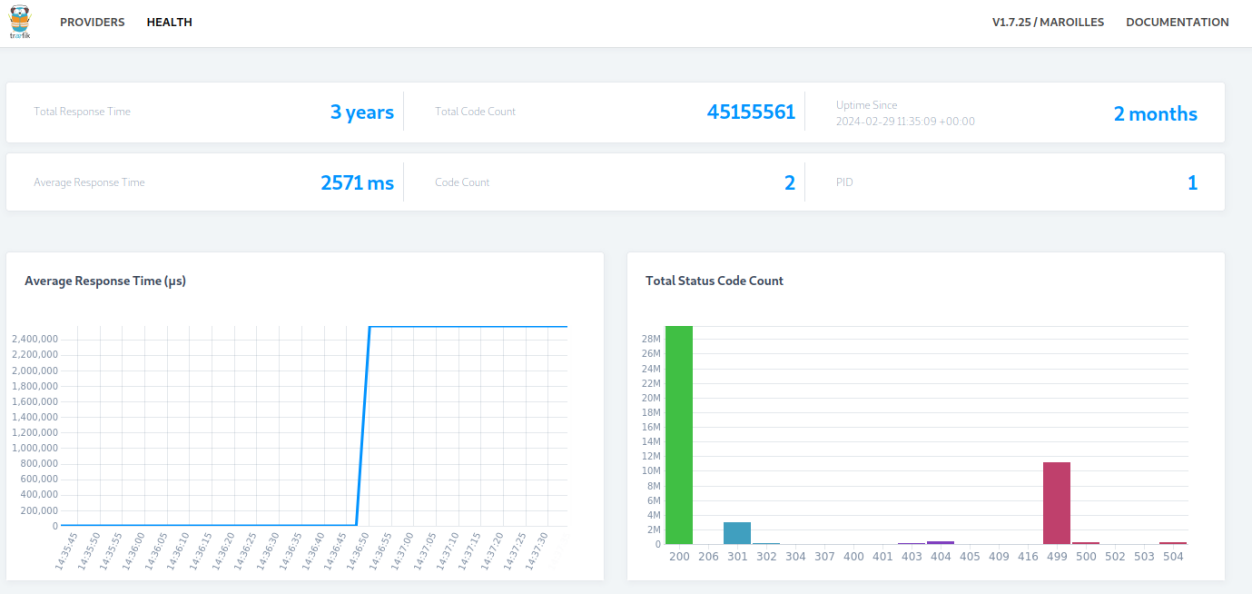
As of 22 April 2024, the address `178.62.255[.]247` hosts on port 8080 a Traefik interface, an HTTP reverse proxy, and load balancer that makes deploying microservices easily. This tool is available in open source on GitHub. It seems that **this control panel is intended to manage several disinformation websites in parallel**, and therefore set up and maintained by the creators of the DoppelGänger campaign. Access to the interface is direct and requires no authentication.



*Screenshot of **http://178.62.255[.]247:8080/dashboard/** page*

On the “Providers” tab, this interface manages several domain names, including `newsroad[.]online`. The full list of managed websites is summarised in *Appendix: Websites referenced in Traefik interface*.

Another tab is available in the interface, entitled **“Health”**. This tab provides a page showing various statistics relating to the current state of the server.



*Screenshot of **http://178.62.255.247:8080/dashboard/status** page*

This dashboard provides an **overview of the server's response time to requests.** The "Total Status Code Count" graph, which illustrates the audience of the websites managed, reveals that since it went live, **the number of consultations has exceeded 26 million**, indicating a level of proliferation considered to be high. This number seems consistent with the reach of the DoppelGänger campaign on social media. For instance, AI Forensics found that between August 2023 and March 2024, pro-Russian political ads linked to DoppelGänger reached over 38 million accounts in France and Germany.

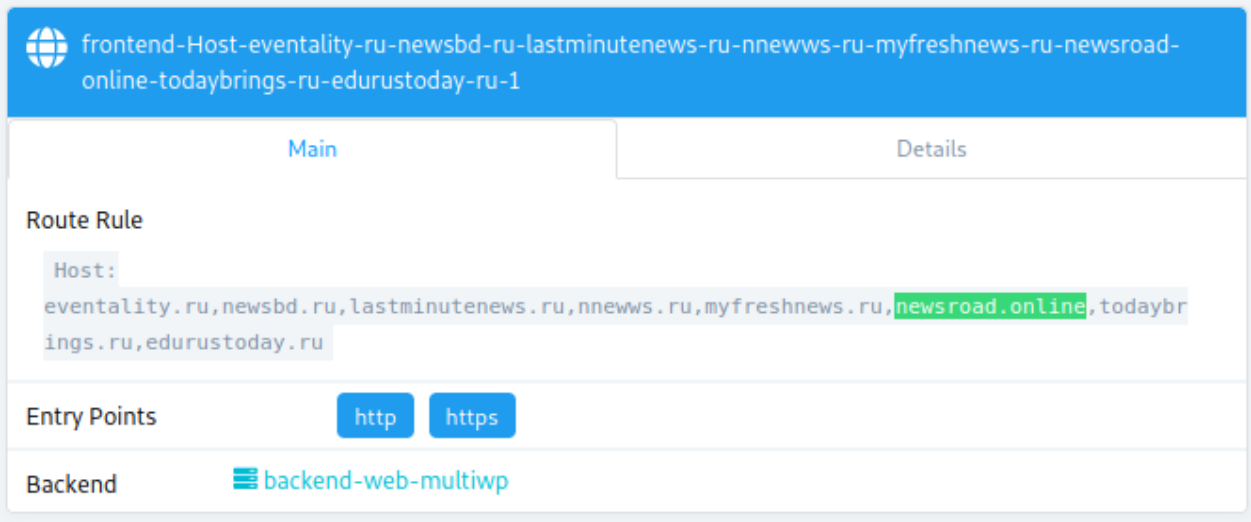
In addition, a table is presented listing all the logs classified under the "error" indicator. This feature enables **real-time observation of interactions with all the websites** listed in the "Providers" tab. This functionality is essential for monitoring performance and identifying potential malfunctions within the managed network.

The URL **/health** provides access to the same data as that available via the **/dashboard/status** interface, but presented in a structured JSON format.

Since this data is accessible via an API returning a response structured format, it is possible to develop a script designed to be executed over several hours to compile an overview of the logs. Analysis of this data revealed that certain articles, which no longer exist, are still being requested (for example /vysokie-tehnologii/kto-poluchit-hyperos-v-yanvare-nazvany-xiaomi-redmi-i-poco/), suggesting the **existence of still active links shared on social networks and likely to be clicked on** by users. In addition, an IPv4 address, `206.189.243[.]184`, which does not appear among the interface elements on Traefik, was identified. This IP address broadcasts the same content as `178.62.255[.]247`, suggesting that it could function as a redundancy solution. As a result, the same script was run to try to discover new data in the logs, but no difference was found.

Uncovering new disinformation websites targeting Russia

An analysis of websites that share the same “Route Rule” for Traefik frontends and backends as `newsroad[.]online` reveals that they use **similar container structures, although the disseminated content differs.** This observation highlights a uniformity in the architecture of these sites, while allowing for diversity in the information presented.



*Screenshot of the **178.62.255[.]247** interface “Provider” tab*

In this way, it is fairly easy to administer these different websites from a technical point of view.

Website	Yandex Metrika counter	Creation date
`newsroad[.]online`	88289747	2022-04-06
`newsbd[.]ru`		2022-03-18
`nnewws[.]ru`		2022-03-10
`lastminutenews[.]ru`		2022-03-10
`eventality[.]ru`		2022-03-10
`myfreshnews[.]ru`		2021-07-12
`edurustoday[.]ru`		2020-05-13

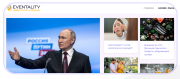
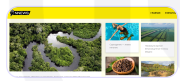
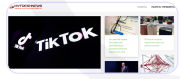
According to VIGINUM, these websites were operational during the period of “increased manoeuvring” identified as June to September 2022. In addition, for sites such as `eventality[.]ru` and `lastminutesnews[.]ru`, we note the use of `urlbox[.]online` at the second level, which is used to generate shortened URLs redirecting to legitimate journalistic sites.

Analysing second level redirection

The **urlbox[.]online** URLs contain a campaign identifier (campaign ID), as it was the case in the request of stage-2 to stage-3 websites described in Section II: Active Infrastructure: a multi-layer mechanism.

Sekoia analysts identified four campaign IDs written in Russian: “**Prez**”, which redirects to articles about the 2024 Russian presidential election, “**Protch**”, which redirects to articles about Russian regions, “**Mat**”, which redirects to articles about “Russkiy Mir”, i.e. Russian values and identity, and “**LDNR**”, which redirects to articles about the Donetsk People’s Republic (DPR) and the Luhansk People’s Republic (LPR). It enables Sekoia to assess that this cluster is dedicated to Russian-speaking propaganda missions, differing from what was previously observed.
A detailed analysis of the content of these websites is presented in the table below:

sekoia | Content analysis of Russian disinformation websites

Preview	Websites	Second-stage website *urlbox[.]online*	Language(s)	Tab theme(s)	Presence of political content
	eventality[.]ru	Yes, redirected to campaigns ID "Prez"	Russian	Business, Markets	Yes
	newsbd[.]ru	No	Russian, English	Lifestyle	Yes
	lastminutenews[.]ru	Yes, redirected to campaigns ID "Protch", "Mat", and "LDNR"	Russian	Economy, Tourism	Yes
	nnewws[.]ru	No	Russian	Economy, Finance	Minor
	myfreshnews[.]ru	No	Russian	Taxes, Management	Minor
	newsroad[.]online	No	Russian, French, English, Deutsch, Italian, Spanish, Ukrainian	None	Minor
	edurustoday[.]ru	No	Russian	Culture	Minor

Although these sites date back to a period of activity in 2022, **they are continually updated and are still publishing content in 2024**. This consistency of updating leads Sekoia analysts to conclude with a high level of confidence that this campaign is still active, and believe that Russian disinformation platforms actively maintain and develop internal narratives in order to continue to engage the Russian population, while countering narratives opposed to the war.

This necessity is part of the management of public opinion in the face of geopolitical developments likely to influence the perception of the conflict. This strategy aims to preserve cohesion and support within the Russian society in the face of external influences that could undermine the government’s official position.

Comparison with Portal Kombat, and the "-news[.]ru" ecosystem

This cluster targets Russian-speaking audiences in Russia and in Ukraine, as demonstrated by the campaign IDs. Therefore, Sekoia analysts **searched for potential overlaps with Portal Kombat**, which is an influence campaign attributed to Russia. Documented by VIGINUM in February 2022, Portal Kombat also targets Russian-speaking audiences, leveraging the "-news[.]ru" ecosystem.

Similarities arise, such as the targeted audience, the redirection to articles written by Russian news outlets agencies, such as Lenta.ru, and the content of websites, which varies from websites sharing political content and others redirecting almost exclusively to non-political articles. Despite these common points, **technical investigations did not enable Sekoia to link the two infrastructures together**. The shared favicon is different from the cluster uncovered by Sekoia, as well as the IPv4 range of "-news[.]ru" (78.21.15.0/24), which differs, leading therefore to a distinct autonomous system (AS 49352).

Therefore, Sekoia assesses this new **DoppelGänger cluster and Portal Kombat are two ongoing, simultaneous yet distinct, Russian influence campaigns with constantly active infrastructures**. However, there is no evident overlap between those two, meaning it might be conducted by different operators in parallel.

Conclusion

The DoppelGänger influence campaign attributed to Structura and SDA, two Russian entities, is characteristic by its large scale, its multi-platform nature, as well as its capacity to adapt its narratives to different countries and the current news.

Following reports published in 2023 about this disinformation campaign by VIGINUM and Recorded Future, Sekoia analysts were able to **confirm that the technical infrastructure of the campaign is still active** and that it is **related to a previously unreported cluster**, managing news websites redirecting towards Russian news outlets. This is consistent with the fact that Structura and SDA are also likely to conduct Russian-speaking campaigns for the Russian government.

Regarding infrastructure uncovered in previous reports, we observed several hundreds of domain names and websites associated with the DoppelGänger infrastructure but it's very likely that part of the infrastructure, notably the one linked to disinformation campaigns on Facebook, remains to be discovered. At this stage of our investigation, it constitutes **a limitation** of our monitoring regarding the campaign evolution over time.

However, Sekoia analysts assess it is likely **the DoppelGänger campaign will remain largely active** for several months, or even years to come. Indeed, while it was uncovered as early as May 2022 and investigation reports illuminating its technical infrastructure were released, the campaign is still active in numerous countries. AI Forensics assessed in a 2024

report that the reach of Facebook's political ads linked to DoppelGänger since their investigation from August 2023 to March 2024 has even increased by five to ten times over time.

The persistence of pro-Russian influence campaigns is likely due to social media platforms failing to efficiently enforce their regulatory policies. But it can also be related to institutions, which are slow to adopt measures following the publication of investigation reports.

Even if the impact of disinformation campaigns is difficult to assess, the increasing **sophistication of DoppelGänger is certain**. It is demonstrated by the **expansion** of the campaign to new platforms, especially video-sharing ones like TikTok and Instagram, which was coupled with the use of deepfakes. Contents also appear increasingly **professional**, mimicking graphic charter of conventional media, or making fake round tables of experts on Youtube. Even if the substance of the narratives remains easily associated with Russian propaganda in most of the cases, an IPSOS survey in France revealed 66% of those questioned believe in at least one piece of fake news presented to them. The recent electoral outcome in Slovakia also questioned the current impact of pro-Russian influence campaigns in shaping public opinions, especially in electoral periods.

The Digital Service Act (DSA) implemented in November 2023 and the Commission guidelines to assist Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) in mitigating risks like election integrity may play a role in urging platforms to prevent the spread of disinformation and also support civil society and government agencies' efforts in protecting the democratic process.

Observables

The list of Observables are available on Sekoia GitHub repository.

Thank you for reading this blogpost. We welcome any reaction, feedback or critics about this analysis. Please contact us on tdr[at]sekoia.io.