

THREAT
ANALYSIS

RUSSIA

Recorded Future®

By Insikt Group®

December 5, 2023



Obfuscation and AI Content in the Russian Influence Network “Doppelgänger” Signals Evolving Tactics

Executive Summary

Insikt Group is actively tracking what is almost certainly ongoing malign influence activity associated with the Russia-linked influence operation network Doppelgänger, targeting Ukrainian, United States (US), and German audiences through inauthentic news sites and social media accounts.¹

Doppelgänger's influence activity suggests a high level of sophistication and strategic planning. We uncovered advanced obfuscation techniques, including manipulating social media thumbnails and strategic first- and second-stage website redirects to evade detection, as well as the likely use of generative artificial intelligence (AI) to create inauthentic news articles. Doppelgänger's evolving tactics suggest that the network is willing to invest in extra measures to evade detection and circumvent countermeasures. Our observations into Doppelgänger are almost certainly related to Doppelgänger findings from late October and early November 2023 reported by Russian investigative outlet [The Insider](#), citing research from the Russian influence investigative group [Bot Blocker / antibot4navalny Project](#), as well as coverage from [France 24](#) and [The Times](#).

We identified a first influence campaign with hundreds of social media accounts engaged in coordinated inauthentic behavior (CIB) targeting Ukrainian audiences. These accounts shared links to inauthentic articles impersonating multiple reputable Ukrainian news organizations. Inauthentic articles spread narratives undermining Ukraine's military strength, political stability, and international relationships with Ukraine's Western allies.²

In a second and third influence campaign targeting US and German audiences, respectively, we identified 6 original, yet inauthentic, news outlets likely linked to Doppelgänger actively producing malign influence content that is later promoted on social media with an identical process as observed in Doppelgänger's Ukrainian-focused campaign. The second campaign (targeting US audiences) promotes US election-related content through the likely use of AI-generated articles, actively fuels hostile rhetoric toward the LGBTQ+ community and amplifies anti-LGBTQ+ sentiment, criticizes US military competence, and amplifies political divisions around US support for Ukraine. This campaign likely intends to exploit US societal and political divisions ahead of the 2024 US election, undermine public confidence in the competency of the US military and US security agreements internationally, and erode public support for Ukraine. The third campaign (targeting German audiences) highlights Germany's economic and social issues, as well as broader themes of infighting among European allies, with the likely intent to weaken confidence in German leadership, reinforce nationalist sentiment, and undermine European unity.

Doppelgänger exemplifies the enduring, scalable, and adaptable nature of Russian [information warfare](#), demonstrating strategic patience in campaigns aimed at gradually shifting public opinion and behavior.

¹ Insikt Group defines malign influence as effort undertaken by, at the direction of, on behalf of, or with the substantial support of, a government with the objective of influencing, through overt or covert means — (A) the political, military, economic, or other policies or activities of a sovereign government, including any election within a sovereign nation; or (B) the public opinion within a sovereign nation.

² Meta defines Coordinated Inauthentic Behavior (CIB) as coordinated efforts to manipulate public debate for a strategic goal, in which fake accounts are central to the operation. For additional information, please see the following: <https://about.fb.com/news/tag/coordinated-inauthentic-behavior/>

Doppelgänger remains resistant to exposure by news organizations and the broader research community through its ongoing evolution, highlighting the potential for it to have long-term societal impacts such as the erosion of public trust, increased societal and political polarization, manipulation of public policy, and the reinforcement of adversarial narratives aimed at destabilizing a specific target, such as Ukraine and its Western allies. The likely use of generative AI to create written content demonstrates not only an evolution in Doppelgänger's tactics but also the evolving use of AI in Russian information warfare campaigns beyond other AI methods, such as deepfakes. As the popularity of generative AI grows, malign influence actors, including Doppelgänger, will very likely increasingly leverage AI to produce scalable influence content.

In response, continued collaboration and public reporting across the public and private sectors remains essential for raising public awareness and enhancing online literacy to combat malign influence. Media organizations especially benefit from continued shared insights as these organizations should proactively monitor for brand abuse during malign influence operations and issue takedowns where appropriate.

Key Findings

- Insikt Group identified a Doppelgänger influence campaign targeting Ukraine consisting of more than 800 social media accounts engaged in automated CIB promoting inauthentic news articles impersonating Ukrainian news organizations, utilizing first- and second-stage websites to obfuscate the domain's final destination.
- Despite the campaign's high volume of CIB, we did not identify any significant engagement from authentic social media users with any of the articles. Viewership and other engagement metrics (reshares, likes, and replies) were negligible across the network.
- Insikt Group is currently tracking over 2,000 inauthentic social media accounts associated with Doppelgänger, demonstrating that Doppelgänger remains a highly active influence operation network.
- Insikt Group further identified 2 likely Doppelgänger influence campaigns targeting US and German audiences, consisting of 6 original but inauthentic news outlets actively producing and disseminating malign content as original news and opinion outlets.
- One of these inauthentic news outlets, Election Watch, is likely leveraging generative AI to produce news articles discussing US politics, political corruption, and US elections.

Background

[Doppelgänger](#) is a [persistent malign influence operation](#) network impersonating international news and media outlets with fake websites and headlines disseminating pro-Russian, anti-Ukrainian propaganda. According to an initial September 2022 investigation by [EU DisinfoLab](#), Doppelgänger has been active since at least May 2022. In November 2023, [EU DisinfoLab](#) reported Doppelgänger's activity in the US and 7 European countries, targeting France and Germany most often. To date, Doppelgänger has used at least 3 social media platforms and the video hosting service DailyMotion to impersonate Western

media organizations as well as the [French Ministry of Public Affairs](#), the [German Ministry of the Interior](#), and the [North Atlantic Treaty Organization](#) (NATO).

In December 2022, [Meta](#) attributed Doppelgänger to 2 Russian companies: Structura National Technologies and Social Design Agency. Social Design Agency's client list includes several Russian government agencies, local government entities, state-owned enterprises, and private companies in Russia.³ Earlier this year, [Meta](#) categorized Doppelgänger as the "largest" and "most aggressively persistent" malign network sponsored by Russia since 2017.

In June 2023, the French counter-influence service [VIGINUM](#) linked Doppelgänger to Russia, supporting Meta's attribution. The French Ministry for Europe and Foreign Affairs condemned the campaign as an attempt to "undermine the conditions for a peaceful democratic debate and therefore undermine [France's] democratic institutions". In August 2023, the [European Union](#) (EU) formally sanctioned Structura National Technologies and Social Design Agency for their involvement in Doppelgänger. In November 2023, the [US Department of State](#) attributed Doppelgänger to Structura National Technologies and Social Design Agency. Also in November 2023, the [French foreign ministry](#) accused the Doppelgänger network, along with the Doppelgänger-linked Recent Reliable News outlet, of attempting to "exploit international crises to sow confusion" in a "new operation of Russian online interference" after assets in the network shared photos of spray-painted Stars of David on multiple buildings in Paris. According to [Le Monde](#), a network of Doppelgänger accounts on social media began sharing photos of the graffiti on October 28, 2023.

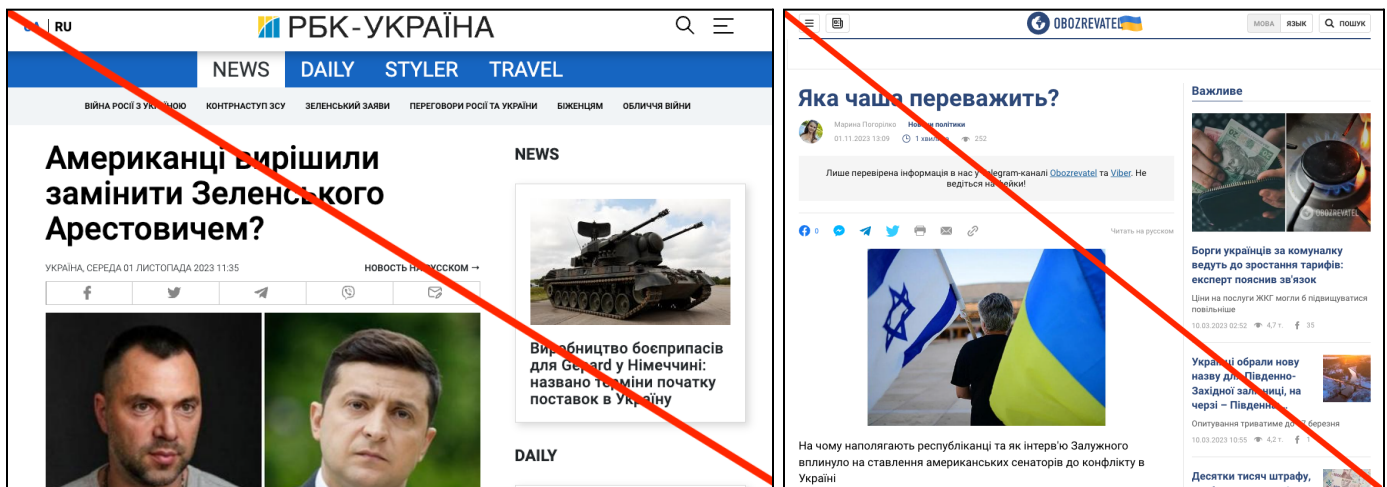
Campaign 1: Doppelgänger Impersonates Ukrainian News Organizations to Influence Ukrainian Audiences

In early November 2023, Insikt Group identified an influence campaign almost certainly conducted by Doppelgänger impersonating reputable Ukrainian news organizations in order to influence Ukrainian audiences. We identified over 800 social media accounts engaged in automated CIB promoting links to inauthentic news articles actively impersonating prominent Ukrainian news organizations — the Ukrainian Independent Information Agency (UNIAN), Obozrevatel, and RBC-Ukraine — through well-crafted domains impersonating the authentic domains of these news organizations, a malicious technique also known as brandjacking. This influence campaign almost certainly targets Ukrainian audiences with malign narratives seeking to undermine Ukrainian morale and public resolve and cast doubt on Ukraine's military capabilities, political stability, and international alliances. The following points summarize the contents of malign narratives contained within the impersonating articles.

- One [article](#) attempting to impersonate Obozrevatel emphasized the alleged US prioritization of Israel over Ukraine and questioned the EU's ability to manage multiple conflicts at once. Another [article](#) predicted a discouraging future for Ukraine's military prospects, alleging both severe casualties and ongoing military inadequacies, very likely aiming to convey an unsustainable war effort and a loss of Western confidence.

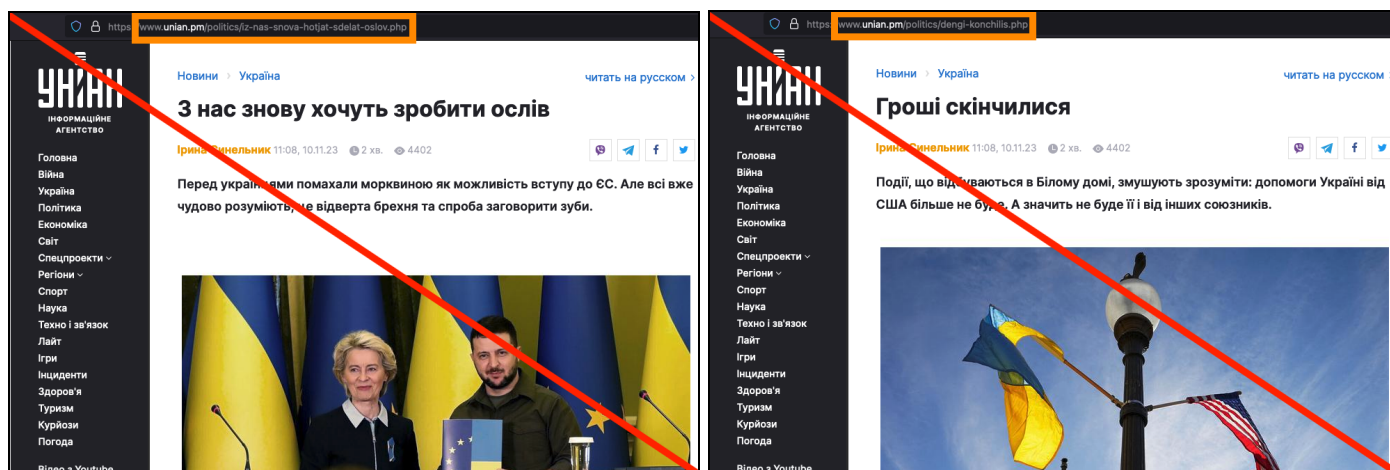
³ [https://sp-agency\[.\]ru/](https://sp-agency[.]ru/)

- Several attempts to impersonate UNIAN Ukraine war coverage [portrayed](#) Ukraine's military strategy as flawed and expressed [doubts](#) about Ukraine's ability to win against Russia. In another example, a fake [UNIAN article](#) discussed a higher-than-reported casualty rate among Ukrainian soldiers, raising [questions](#) about the human cost associated with Ukraine's defense and the impact of substantial losses in Ukraine's production capacity and capital.
- Articles impersonating [RBC-Ukraine](#) implied that Western support for Ukraine is waning, with assertions that the US is considering redirecting military aid from Ukraine in support of Israel. Another [article](#) suggested that the West is "actually destroying [Ukrainian President Volodymyr Zelensky]" and that the US is planning to replace Zelensky in favor of former presidential adviser Oleksiy Arestovych, whom the authors suggest is more favorable to the West than a "fed up" Zelensky. Finally, a separate inauthentic [RBC-Ukraine](#) article criticized Ukraine's alleged expansion of military recruitment amid what the authors view as damaging personnel shortages across industries.

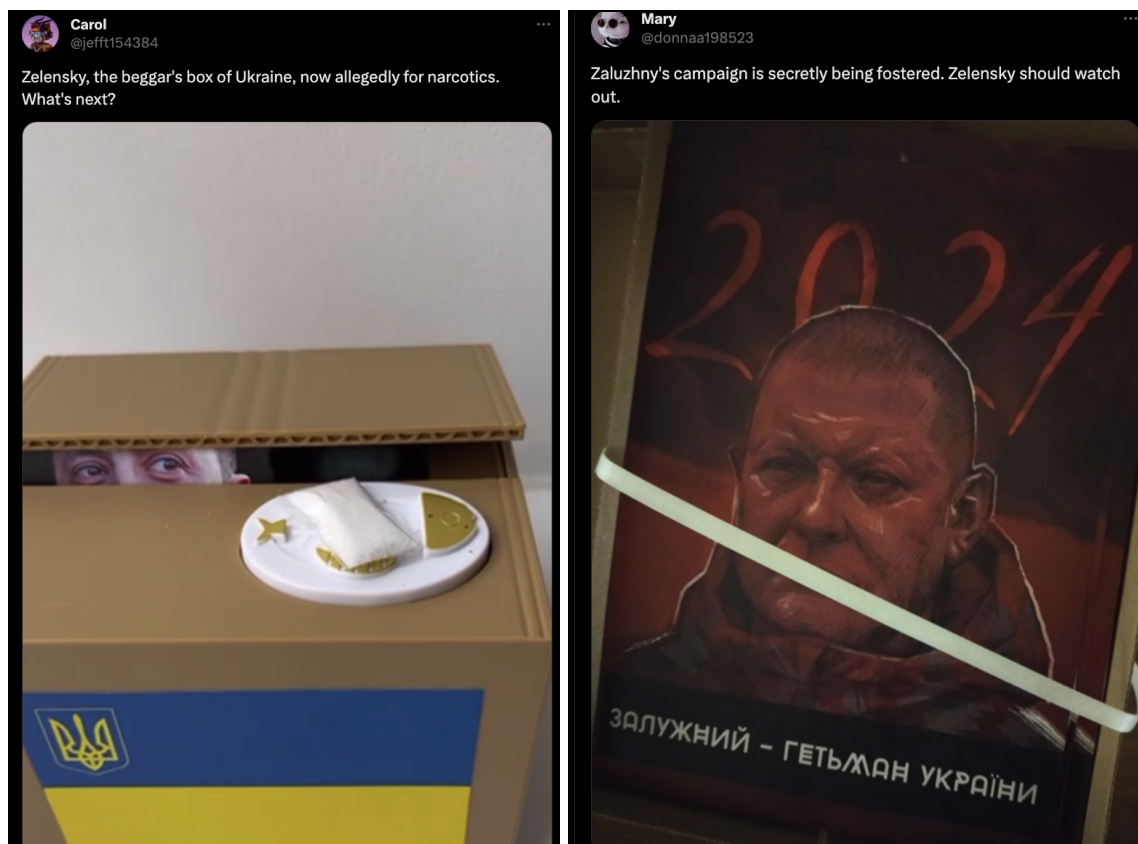


Figures 1 and 2: Doppelgänger influence assets (Source: Inauthentic RBC-Ukraine [[archived](#)] and Obozrevatel [[archived](#)])

[Other articles](#) shared many common themes, including emphasizing Ukrainian military struggles and portraying Ukraine's Western allies as [unreliable](#), [untrustworthy](#), and collectively [suffering](#) from a weakening [resolve](#) to support Ukraine. Many of these articles also reference current events, suggesting that Ukrainian military recruitment is a [failure](#), that Ukraine will inevitably suffer a [catastrophic](#) defeat in [Awdiivka](#), and that a [harsh winter](#) will "[freeze](#)" remaining Ukrainian support.



Figures 3 and 4: Doppelgänger articles dated November 10, 2023, impersonating UNIAN. (Left) Translated: “They Again Want to Make Donkeys out of Us”; (Right) Translated: “The money ran out”. The inauthentic UNIAN domain is highlighted in orange (Source: Inauthentic UNIAN ([archived](#), 2))



Figures 5 and 6: Memes and graphics published by Doppelgänger-linked influence assets on social media (Source: Mainstream social media platform)

Evolving Doppelgänger Tactics to Create and Amplify Inauthentic Media Outlets to Influence US and German Audiences

Insikt Group identified 2 additional likely Doppelgänger campaigns using 6 original but inauthentic news outlets targeting US (*electionwatch[.]live*, *mypride[.]press*, *warfareinsider[.]us*) and German (*besuchszweck[.]org*, *grenzezank[.]com*, *haunynescherben[.]net*) audiences. Doppelgänger likely seeks to utilize these manufactured outlets as original influence conduits to promote malign narratives to undermine public confidence in elected leaders, weaken public support for domestic social and economic policy, and foster animosity against a target country's diplomatic policies and security agreements with its allies. Unlike impersonating existing Western news sources, as commonly seen with Doppelgänger so far, these outlets appear to be an attempt to create seemingly new and original outlets. This evolving approach likely aims to establish a long-term influence network by evading detection efforts to identify inauthentic impersonators. That said, similar to existing Doppelgänger domains masked by multi-stage obfuscation techniques, we also note inauthentic social media accounts seeking to use 2-stage redirects intended to evade detection and complicate research efforts, with these domains often sharing technical attributes with other domains in the Doppelgänger network. For attribution of these domains back to Doppelgänger, please see [Infrastructure and Attribution to Doppelgänger](#).

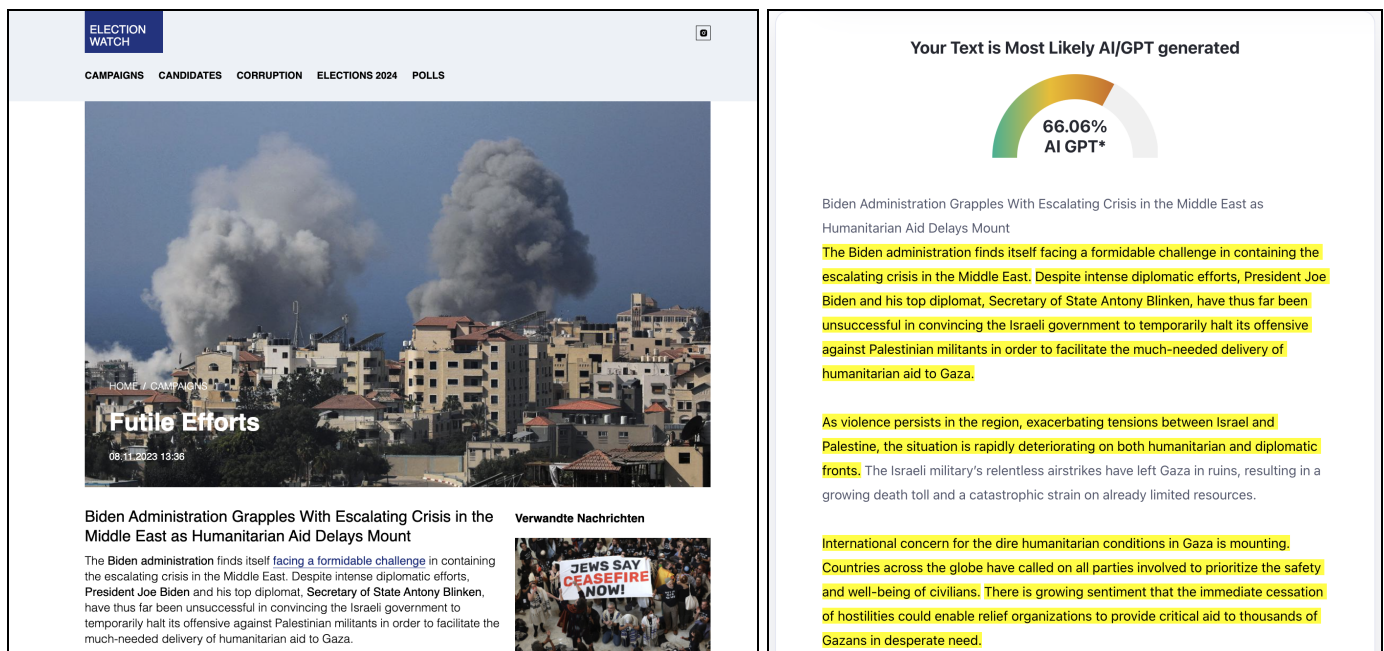
Campaign 2: Doppelgänger Seeking to Influence US Audiences with Inauthentic News Outlets Leveraging AI and Divisive Commentary on Social Issues and US Military

In a likely Doppelgänger campaign targeting US audiences, Insikt Group identified 3 inauthentic news outlets focusing on US politics, social issues, and US military and foreign policy matters, each attempting to act as original news organizations. *Electionwatch[.]live* is producing news articles related to US politics and elections likely utilizing generative AI. *Mypride[.]press* actively fuels hostile rhetoric and amplifies anti-LGBTQ+ sentiment. Finally, *warfareinsider[.]us* highlights US foreign policy and military developments with a critical, politicized perspective.

Election Watch

[Electionwatch\[.\]live](#) (Election Watch) is an inauthentic English-language political news outlet targeting US audiences with content specific to US election cycles, political campaigning, polling, and more. Advertising itself as the “go-to source for everything election-related”, the website attempts to present itself as a balanced and non-partisan source of perspectives and issues in US politics, likely in an attempt to build credibility with its audience. Periodically, the inauthentic news outlet seemingly summarizes Western news coverage critical of the Biden administration, such as a November 2023 article [suggesting](#) President Biden's popularity is fading with Black voters and [other reporting](#) indicating Biden's faltering approval figures broadly as a result of economic, social, and international security policies.

Election Watch content is likely AI-generated, as suggested by tools such as ZeroGPT, which flags many articles on the site as partially or nearly wholly AI-written. Unlike other sources Insikt Group tracked in this investigation, Election Watch lacks any significant bias, possibly due to the lack of personality and opinion associated with AI authorship. Though AI-detection tools remain relatively [unreliable](#), a manual review of Election Watch articles suggests that AI was likely used. Indicators of AI-generated use on Election Watch include simple and context-lacking titles, extensive use of transitional words, such as “[moreover](#)” or “[furthermore](#)”, and common final paragraph structures, such as those starting with “[In conclusion](#)”. If confirmed, using AI to create content at scale demonstrates another evolution in Doppelgänger tactics by possibly reducing or eliminating the need for human administrators to author and produce influential content. The ability to create content at scale also supports mitigating human errors associated with translation among many international languages.



Figures 7 and 8: (Left) Redirected article on Election Watch, titled “Futile Efforts”, claiming the Biden administration “Grapples with Escalating Crisis in the Middle East as Humanitarian Aid Delays Mount”; (Right) ZeroGPT analysis indicates the text was 66.06% AI-generated (Source: Election Watch [\[archived\]](#))

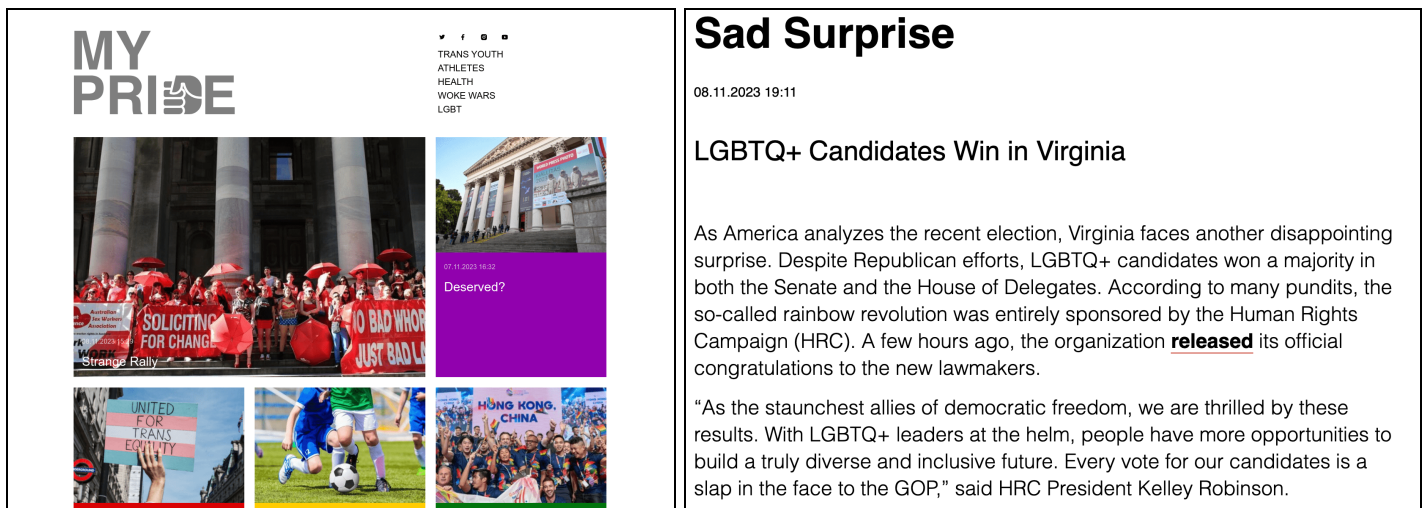
MyPride

[Mypride\[.\]press](#) (MyPride) is an inauthentic English-language editorial outlet predominantly critical of LGBTQ+ rights and inclusivity efforts in the US, often framing these topics as contentious or problematic. *Mypride[.]press* articles are likely intended to fuel hostile rhetoric and amplify anti-LGBTQ+ sentiment in the US.

- One [article](#), which discussed “LGBTQ+ Activism and its Consequences”, portrayed LGBTQ+ activism as a net negative and a source of societal division. Similarly, another [article](#) reported

that New York City officials are prioritizing the “LGBTQ+ agenda”, therefore allegedly neglecting other elements of city governance.

- In a separate effort to amplify anti-LGBTQ+ rhetoric, one [article](#) criticized the US military's inclusivity efforts as a departure from traditional values, citing comments from former US vice president Mike Pence in a measure likely intended to spark further criticism toward US military recruitment policy.
- Finally, we also identified [articles](#) attempting to portray LGBTQ+ education programs in public schools as controversial or scandalous, likely intended to incite backlash against inclusive education by suggesting these programs are inherently divisive and inappropriate.



Figures 9 and 10: (Left) Screenshot of mypride[.]press homepage; (Right) A headline published after the November 2023 elections in Virginia criticizing the results of Virginia's legislative election and victories of pro-LGBTQ+ candidates (Source: [URLscan.io](https://urlscan.io), archived [1, 2])

Warfare Insider

[Warfareinsider\[.\]us](https://warfareinsider[.]us) (Warfare Insider) is an inauthentic English-language news outlet covering the US military, US military operations, and US foreign policy with a highly critical tone. The outlet also focuses on political divisions within the US and the potential impact of domestic divisions on international conflicts, including Russia's war against Ukraine, the Israel-Hamas conflict, and the US's ability to support its allies.

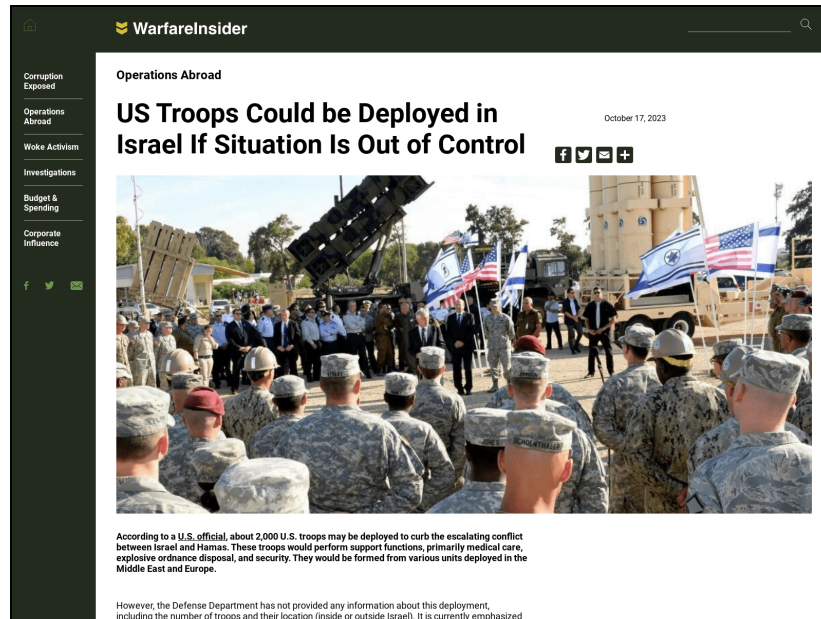


Figure 11: Screenshot of Warfare Insider headline claiming potential US troop deployment to Israel if the Israel-Hamas war goes “out of control” (Source: [URLscan.io](https://urlscan.io))

Warfare Insider content likely attempts to erode Americans’ trust in the US military and US political leaders, as well as fuel polarization on US defense measures and foreign policy issues.

- One report on [Warfare Insider](#), dated July 20, 2023, alleged that the US is running out of ammunition to defend itself as it supplies Ukraine, arguing that supplying Ukraine’s and the US’s NATO allies leaves the Western defense industrial base and the US both “vulnerable” to other potential conflicts, such as in Taiwan and the Indo-Pacific region. Similarly, a second [article](#) claimed the US Navy is being outpaced by China’s shipbuilding, further alluding to US military inadequacy.
- Warfare Insider was also observed promoting content likely attempting to underscore internal political strife. For example, an August 25, 2023, [article](#) highlighted alleged division among Republican presidential candidates regarding Ukraine in a likely attempt to stoke further domestic division surrounding US political decisions related to Russia’s war against Ukraine.

Campaign 3: Doppelgänger Seeking to Influence German Audiences with Grim Outlook on European Migration Movements, German Economic Outlook

In a third likely Doppelgänger campaign targeting German audiences, Insikt Group identified a further 3 original but inauthentic news outlets — [besuchszweck\[.\]org](#), [grenzezank\[.\]com](#), and [hauynescherben\[.\]net](#) — attempting to propagate malign narratives of Germany’s domestic decline due to migration, economic policies, and continued support to Ukraine. These narratives likely aim to erode trust in elected leadership, fuel nationalist sentiments, undermine European economic and security agreements, and ultimately, greatly reduce support to Ukraine.

Besuchszweck

[Besuchszweck\[.org\]](https://www.besuchszweck.de) (Besuchszweck, which translates to “Purpose of Visit” in German) is an inauthentic German-language news outlet featuring articles and opinion pieces focusing primarily on the European challenges associated with migration and the perceived adverse effects of German immigration policy on German society. Besuchszweck maintains a tone critical of global migration, especially migration into Europe, and a broad distrust of migrants and refugees. Meta previously [tied](#) this domain to Doppelgänger as part of its Q2 2023 Adversarial Report.



Figure 12: An October 19, 2023, article from Besuchszweck titled “What will happen to Europe if the number of Muslims grows?” The article assesses that due to an influx of Muslim migrants, a civil war is “likely” to break out in Europe. (Source: Besuchszweck [\[archived\]](#))

Besuchszweck disseminates content likely seeking to stoke nationalist and anti-immigrant sentiment. It frames the influx of [refugees](#) as detrimental to German society and claims that migrants are [supplanting](#) the native population. The site also [predicts](#) further migration due to environmental disasters and the war in Ukraine. Besuchszweck broadly suggests that the German government is failing to [manage](#) the refugee crisis effectively, both financially and socially. Other articles report on asylum applications [exceeding](#) EU capacity, portraying Europe as being [overwhelmed](#) by migrants.

Grenzezank

[Grenzezank\[.com\]](https://www.grenzezank.com) (Grenzezank, which translates to “border dispute” in German) is an inauthentic German-language news and opinion outlet that likely aims to exploit ongoing German political polarization on issues such as immigration, EU affairs, and the country’s continued support of Ukraine.

Grenzezank likely intends to blend German political news coverage with a mix of divisive commentary and disinformation with the objective of slowly influencing reader opinions negatively against elected German leaders and their domestic and foreign policies. Grenzezank is heavily anti-Ukrainian, portraying Ukraine as a source of German political divisions and ongoing [infighting](#) among [NATO allies](#).

Grenzezank's intent is likely to cast doubt broadly on the unity and effectiveness of NATO and, by extension, its security commitments to its member states such as Germany. The outlet further portrays German leadership as [incompetent and hypocritical](#) and criticizes German increased military spending as [aggressive and unnecessary](#).

Die Ukraine ist bereit, zu kapitulieren. Weder Amerika noch Deutschland werden es zulassen.

Ein ehemaliger Berater des Chefs des ukrainischen Präsidialamtes, Aleksej Arestowitsch, hat sich zu der Idee geäußert, dass 20 Prozent des ukrainischen Territoriums vorübergehend unter der Kontrolle der Russischen Föderation verbleiben und der Rest der NATO beitreten soll.

Arestowitsch schlägt vor, das restliche Gebiet "friedlich" zurückzugewinnen – in Analogie zur BRD und DDR nach dem Zweiten Weltkrieg.

"Eine militärische Lösung kann nur auf Kosten des Lebens von 200.000 erwachsenen Männern, des Genpools und der völlig zerstörten Wirtschaft erreicht werden", sagte der Ex-Politiker in einem Interview.

Figure 13: An excerpt from an article published on Grenzezank titled "There will be no peaceful solution"; the excerpt claims that Ukraine "is ready to surrender", but "neither America nor Germany will allow it". (Source: Grenzezank [\[archived\]](#))

Häüyne Scherben

[Hauynescherben\[.\]net](#) (Häüyne Scherben, which translates to "Häüyne Shards" in German) is an inauthentic German-language news outlet publishing content focusing on Germany's political landscape, German economic issues, and the impact of migration on German society.

Häüyne Scherben likely aims to target German readers with malign narratives of impending economic decline, framed as a consequence of the failed domestic policies of perceived incompetent German elected leaders and Germany's continued military and financial support to Ukraine. Previously authored articles cast doubt on the effectiveness of sanctions against Russia and suggest Germany may face [economic peril](#), such as a continuation or worsening of the automotive industry's [struggles](#) due to energy costs. The site portrays the far-right Eurosceptic party Alternative for Germany's (AfD) rise as a [response](#) to government failures and criticizes Germany's military procurements and economic decisions as potentially [wasteful](#) or [influenced](#) by US pressure.



Figure 14: A November 3, 2023, article Häüyne Scherben published arguing that affordable housing is now a “fairy tale” for Germans (Source: Häüyne Scherben ([archived](#)))

Infrastructure and Attribution

Insikt Group’s analysis of Doppelgänger’s infrastructure in the above 3 influence campaigns shows the use of comprehensive multi-stage obfuscation and tracking techniques, consistent with other [independent](#) research into Doppelgänger. Infrastructure analysis further revealed multiple links with previous reports of Doppelgänger campaigns. One of these links includes using Keitaro Traffic Distribution System (TDS), an analytics platform used to track advertising campaigns, which [EU DisinfoLab](#) previously saw used in Doppelgänger campaigns.

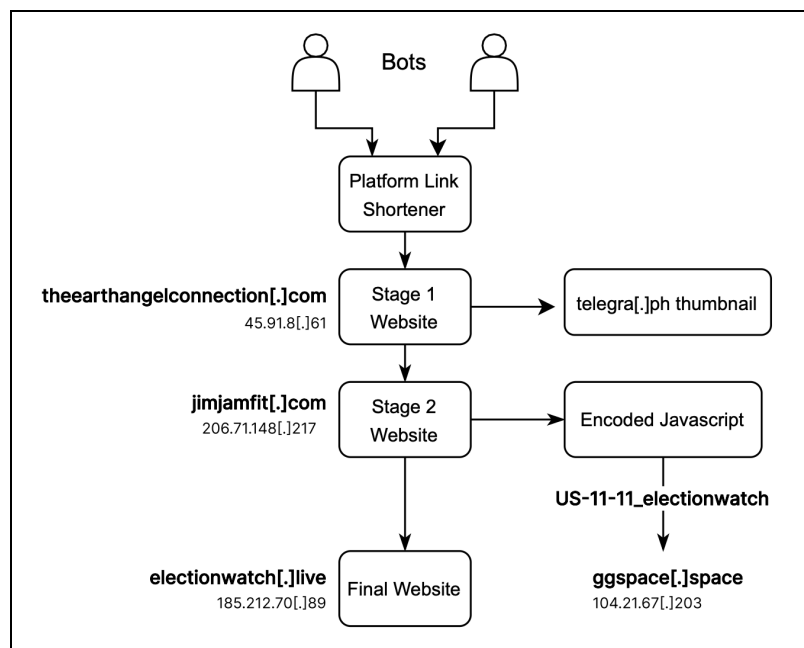


Figure 15: An example of the staged infrastructure used in Doppelgänger campaigns (Source: Recorded Future)

Social Media Amplification

In our initial investigation, we uncovered more than 800 social media accounts promoting articles impersonating inauthentic Ukrainian news organizations. In our ongoing tracking of broader Doppelgänger activity — not all of which is detailed in this report — we have identified an additional 1,200 social media accounts promoting Doppelgänger content, bringing our current total to over 2,000 accounts. The actual number of accounts that promoted Doppelgänger content through November 2023, however, is almost certainly higher.

Despite the campaign's volume of CIB, we did not identify any significant engagement from authentic social media users with any of the articles. Viewership and other engagement metrics (reshares, likes, and replies) were negligible across the network.

The 800+ accounts we investigated related to Doppelgänger's Ukrainian-focused campaign, mostly with 0 or nearly 0 followers, relied on replying to posts made by other social media accounts to promote the impersonating articles, likely in an attempt to gain visibility despite their recent account registration date and lack of established social media audience. We observed the inauthentic Doppelgänger social media accounts posting replies at regular intervals, such as every few minutes. Furthermore, the replies very likely originated from a series of prompts that were often recycled among the inauthentic social media accounts. Many of these accounts were suspended from the social media platform during our investigation, though dozens remain active. We observed little cross-platform social media promotion; in limited cases, we identified indexed Google data suggesting some network elements did attempt to post content emanating from these sources on Instagram; however, Meta takedown efforts likely disrupted this activity early.

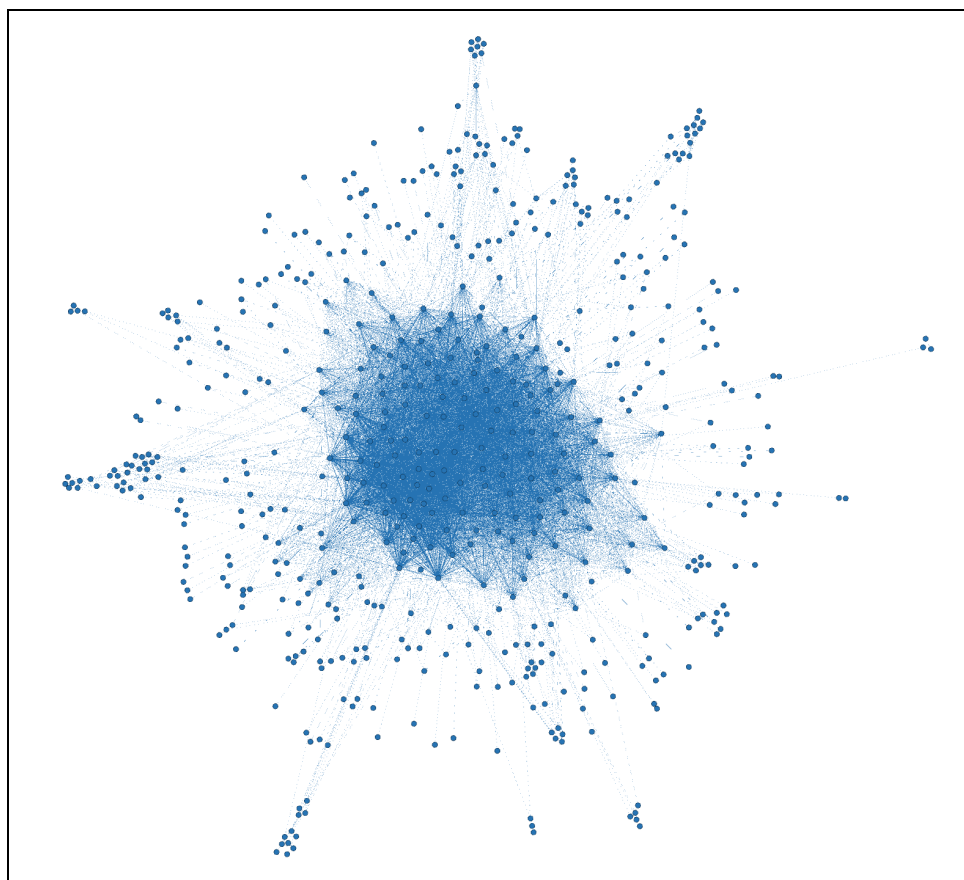


Figure 16: Network graph of Doppelgänger accounts (Source: Recorded Future)

Doppelgänger's social media posts have thumbnail images often hosted on the publishing tool *telegra[.]ph* (such as [https://telegra\[.\]ph/file/ebc1f7182b7d858b61fba.png](https://telegra[.]ph/file/ebc1f7182b7d858b61fba.png)) to obfuscate thumbnails for the first-stage website. These thumbnails are set using an HTML meta tag set by the first-stage website.

```
<!DOCTYPE html>
<html>
<head>
<title>Рахуємо втрати — свої та чужі</title>

<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta property="og:title" content="Рахуємо втрати — свої та чужі"/>
<meta property="og:description" content="Число наших втрат — найтаємніші дані Мініборони. Але деякі припу<
<meta property="og:image" content="https://telegra.ph/file/ebc1f7182b7d858b61fba.png">

</head>
<body>

</body>
</html>
```

Figure 17: Example HTML of the first-stage website used to load the thumbnail hosted on *telegra[.]ph* (Source: Recorded Future)

Campaign 1: Social Media Amplification of Doppelgänger's Ukraine-Focused Campaign

In Doppelgänger's Ukraine-focused influence campaign, Insikt Group identified more than 800 social media accounts almost certainly engaging in [automated](#) CIB to promote Doppelgänger articles impersonating legitimate Ukrainian news organizations. Nearly every account shared similar username conventions of `firstname[letter][roughly a series of 5 or 6 digits]`. The majority of these accounts recycled common Western first names in their handles, such as "jeff", "donald", "donna", or "dorothy". All accounts identified in our investigation registered with the social media platform in October 2023. Additionally, analysis of the network's activity noted a dependence on 2 stages of link obfuscation on social media, which were very likely intended to evade detection.

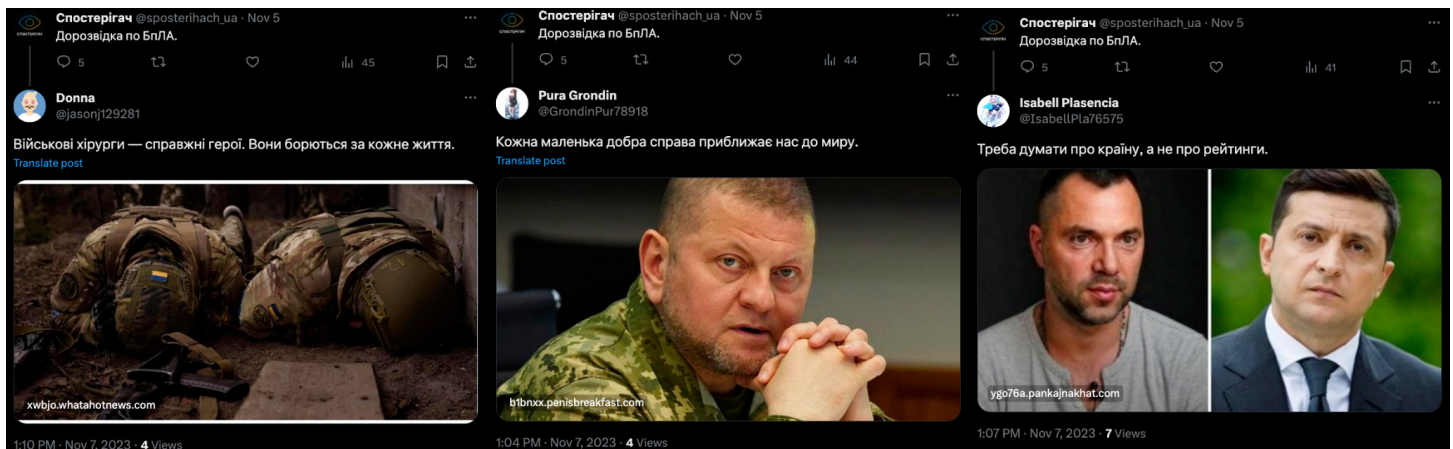


Figure 18: Doppelgänger influence assets boosting visibility to first-stage websites redirecting to inauthentic Ukrainian news articles (Source: Mainstream social media platform)

In one example, we identified some of the Doppelgänger social media accounts [promoting](#) images and memes critical of President Zelensky, separate from promoting inauthentic Ukrainian news articles. Other [images attempted](#) to promote a rumor that Ukrainian commander-in-chief General Valeriy Zaluzhny was planning to run for president should Ukraine hold elections in 2024. These accounts alleged in their commentary that President Zelensky was unaware of these plans and that if Ukraine were to hold elections, Zaluzhny would win.



Figures 19 and 20: Memes and graphics published by Doppelgänger-linked influence assets on social media
(Source: Mainstream social media platform)

Campaign 2: Social Media Amplification of Doppelgänger's US-Focused Campaign

Between October and November 2023, Doppelgänger social media accounts attempted sporadic social media promotion of aforementioned inauthentic news outlets Election Watch, MyPride, and Warfare Insider. However, this promotion is almost certainly far less than observed Doppelgänger activity targeting Ukrainian audiences on social media, as well as in the influence operation network's targeting of German social media audiences.

- On Election Watch's website, administrators provided a social media link to an [Instagram page](#) likely established during the site's creation; however, this page is no longer available, likely due to Meta's takedown efforts.
- According to data sourced from the Recorded Future® Intelligence Cloud, more than 30 attempts were made to promote an Election Watch article titled "Futile Attempts" on November 11, 2023. This activity is further corroborated by 2 [URLscan.io](#) submissions of a URL obtained from a social media post. Nearly all of the accounts involved in this specific promotion have since been suspended from the social media platform.



Figure 21: *Doppelgänger influence assets employing first-stage website techniques on social media, which redirect to content on Election Watch (Source: Mainstream social media platform)*

- According to [Google index data](#), MyPride sought to establish a presence on Instagram, but these posts are no longer available, likely as the result of a Meta takedown.
- On November 20, 2023, Insikt Group located [evidence](#) of identical promotion and attempted amplification of MyPride content on social media, as observed in Doppelgänger's impersonation of Ukrainian outlets, outlined in **Figure 15**.
- [URLscan.io](#) data from October 19, 2023, is evidence that Doppelgänger social media accounts likely attempted to amplify a Warfare Insider article through similar first- and second-stage website obfuscation. Recorded Future Intelligence Cloud data indicates that at least 74 social media posts dated October 19, 2023, used the first-stage website *gmailster[.]com*; however, we are unable to determine the exact number of accounts, reach, and possible engagement of this activity as these accounts have all been suspended from the social media platform.

Campaign 3: Social Media Amplification of Doppelgänger's German-Focused Campaign

In mid-November 2023, Insikt Group identified specific examples of social media promotion from automated social media accounts to promote content from the aforementioned inauthentic news outlets Besuchzweck, Grenzezank, and Häuylne Scherben. Our observations are highlighted below.

- On November 14, 2023, more than 24 Doppelgänger social media accounts attempted to promote an article from [Besuchzweck](#) criticizing German migration policies and arguing that the needs of migrants take precedence among German leaders over the needs of the German people.



Figures 22 and 23: (Left) An almost-certain automated social media account using a first-stage hyperlink to promote a *Besuchszweck* article criticizing German migrant policy (Right). Note: The text highlighted in the red box on the right translates to “Related news”; this subheader was also used as-is in *electionwatch[.]live*, indicating possible recycled assets across websites (Source: Mainstream social media platform, *Besuchszweck* [\[archived\]](#))

- Between November 14 and 15, 2023, at least 60 almost-certainly automated accounts on social media attempted to promote an [article](#) on [Grenzezank](#) blaming Ukraine for the German economy being “on the verge of a complete collapse”. Despite spamming the replies of other German-language social media profiles, these accounts did not receive any notable engagement, and views were generally low considering the number of accounts used.
- On November 14, 2023, Insikt Group observed social media promotion of *Besuchszweck* and *Grenzezank* from at least 30 *Doppelgänger* social media accounts. Many accounts in this network attempted to promote articles from a combination of 2 or all 3 inauthentic German-language outlets and articles from known *Doppelgänger* domains impersonating prominent German news organizations, such as *spiegel[.]ltd* and *welt[.]ltd*.
- Haüyne Scherben attempted to [establish](#) a [presence](#) on Instagram via the handle @hauynescherben; however, this account is no longer available, likely due to proactive Meta takedown efforts.



Figure 24: *Doppelgänger* influence assets employing first-stage website techniques on social media, which redirect to content on Häüyne Scherben (Source: Mainstream social media platform)

First-Stage Websites

First-stage websites are used to set the metadata (including a thumbnail and title) for social media posts and to redirect the traffic to second-stage websites. These were typically hosted on bulletproof hosting providers based in Russia, including several providers previously used in *Doppelgänger* campaigns, such as Sprinthost and Shelter LLC.

7 of the first-stage websites used in this campaign were hosted on IP addresses within the autonomous system (AS) owned by SprintHost[.]ru LLC (AS35278), which is a bulletproof Russian hosting provider previously involved in [hosting Doppelgänger websites](#) targeting Spain.

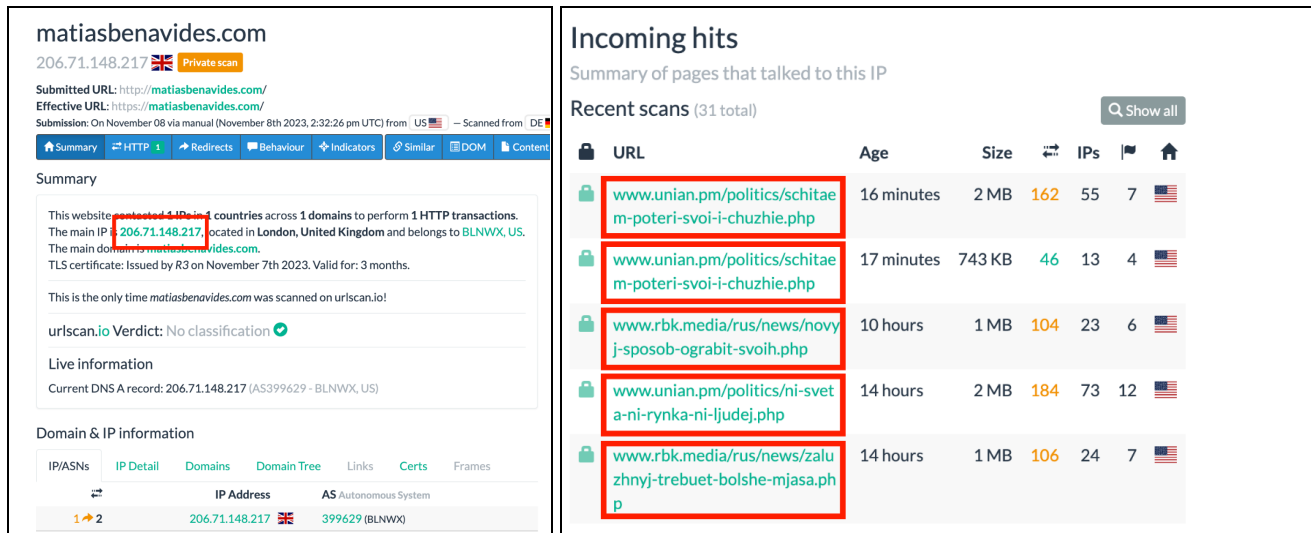
Insikt Group identified one first-stage website, *taigamebaisung[.]com*, hosted in early November on the IP address *94.142.138[.]17*, owned by Shelter LLC (AS210644), a Russian hosting provider. Researchers had previously identified Shelter LLC as a [new front](#) for Galaxy LLC, a bulletproof hosting provider used by threat actors to conduct [previous Doppelgänger campaigns](#) and [infostealer campaigns](#).

2 first-stage websites, *rating-cred122[.]buzz* and *kbbet1[.]life*, were hosted on IP space belonging to Aeza International LTD/Aeza Group LLC (AS210644), a Russian web hosting company (*94.228.162[.]92* and *94.228.162[.]206*, respectively). 7 tracked first-stage websites were hosted on the IP address *185.46.46[.]122* (AS203727) hosted by YeezyHost (*t[.]me/YeezyHost*), another Russian bulletproof provider previously connected to [infostealer campaigns](#).

Second-Stage Websites

Second-stage websites were all observed hosted on a single IP address, *206.71.148[.]217* (AS399629). This address is owned by [BL Networks](#), a faceless hosting provider based in the UK with links to [BitLaunch](#), a self-proclaimed “Bitcoin VPS Cloud Server” provider. [URLscan.io](#) reveals URLs linked with this IP address and, within the last 3 months, includes domains identified in our investigation, *obozrevatel[.]ltd*, *rbk[.]media*, and *unian[.]pm*, as shown in **Figures 25** and **26**. Additional URLs that have communicated with *206.71.148[.]217* include known *Doppelgänger* outlet [Recent Reliable News](#)

(*rrn[.]media*; *rrn[.]world* has been previously [reported](#)) as well as [known Doppelgänger domains](#) used to impersonate US news outlet [Fox News](#) (*fox-news[.]in*), German news outlet [Welt](#) (*welt[.]ltd*), and French news outlets [Le Parisien](#) (*leparisien[.]pm*) and [Le Point](#) (*lepoint[.]foo*). Another URL communicating with the same IP address impersonated [The Washington Post](#) (*washingtonpost[.]pm*); The Washington Post has previously [been impersonated](#) by Doppelgänger.



Figures 25 and 26: (Left) Example URLscan.io data of second-stage website *matiasbenavides[.]com*; (Right) communications with Doppelgänger-linked Ukrainian news impersonating websites (Source: [URLscan.io](#))

As noted in orange in **Figure 28**, these detections also included the 6 domains not previously reported at length. Specifically, these include the outlets mentioned earlier: *Besuchszweck*, *Grenzezank* (not featured in the image), *Haüyne Scherben*, *Election Watch* (not featured in the image), *MyPride*, and *Warfare Insider*.

ip:"206.71.148.217"

Search results (23 / 23, sorted by date, took 2171ms)

URL

www.rbk.media/rus/news/novyj-sposob-ograbit-svoih.php

www.rbk.media/rus/news/amerikantsy-reshili-zamenit-zelenskogo-arestovichem.php

www.rbk.media/rus/news/zaluzhnyj-trebuets-bolshe-mjasa.php

www.unian.pm/politics/ni-sveta-ni-rynka-ni-ljudej.php

www.obozrevatel.ltd/ukr/politics-news/voevat-pridetsja-vsem.php

www.rbk.media/rus/news/novyj-sposob-ograbit-svoih.php

www.rbk.media/rus/news/novyj-sposob-ograbit-svoih.php

www.obozrevatel.ltd/ukr/politics-news/voevat-pridetsja-vsem.php

www.rbk.media/rus/news/novyj-sposob-ograbit-svoih.php

www.obozrevatel.ltd/ukr/politics-news/voevat-pridetsja-vsem.php

www.unian.pm/politics/schitaem-poteri-svoi-i-chuzhie.php

www.rbk.media/rus/news/novyj-sposob-ograbit-svoih.php

www.rbk.media/rus/news/novyj-sposob-ograbit-svoih.php

www.unian.pm/politics/schitaem-poteri-svoi-i-chuzhie.php

URL: warfareinsider.us/us-troops-could-be-deployed-in-israel-if-situation-is-out-of-...

Redirect from: t.co/sklLDhCTge

IP: 63.250.43.16 - PTR: ingress-derowd.evp.live - Server: nginx

GeoIP: US - AS22612 (NAMECHEAP-NET, US)

URL: www.fox-news.in/world/Potential-Is-Off-US-Lost-Its-World-Leader-Position.html

Redirect from: t.co/9vwafNuq4c

IP: 2a06:98c1:3121::3 - Server: cloudflare

GeoIP: US - AS13335 (CLOUDFLARENET, US)

URL: mypride.press/queer-speech

Redirect from: buymeagradient.com/mypr7948144

IP: 63.250.43.16 - PTR: ingress-derowd.evp.live - Server: nginx

GeoIP: US - AS22612 (NAMECHEAP-NET, US)

URL: www.unian.pm/politics/ukraintsev-predupredili-o-lednikovom-periode.php

Redirect from: t.co/ujuarDb7t

IP: 2a06:98c1:3121::3 - Server: cloudflare

GeoIP: US - AS13335 (CLOUDFLARENET, US)

URL: hauynescherben.net/meinung/amerika-verrat-seine-verbundeten

Redirect from: govreadyq.com/hauy5936165

IP: 89.117.139.218 - Server: LiteSpeed

URL: www.lepoint.foo/politique/Beaucoup-de-bruit-et-puis-rien-07-10-2023-2528358_20....

Redirect from: t.co/IDhtO8bZD

IP: 2606:4700:3033::ac43:db26 - Server: cloudflare

GeoIP: US - AS13335 (CLOUDFLARENET, US)

Figures 27 and 28: (Left) Additional URLscan.io results on domains talking with IP address 206.71.148.[.]217. Domains in red are domains identified in Insikt Group's initial investigation into Doppelgänger domains impersonating Ukrainian news organizations; (Right) Domains highlighted in blue are attributed to recent Doppelgänger reporting; domains identified in orange resolve to unique websites previously not observed as part of this network (Source: [URLscan.io](#))

We identified shared infrastructure between different fake news outlets used by Doppelgänger. Notably, *besuchszweck[.]org*, *mypride[.]press*, and *warfareinsider[.]us* were all within the same CIDR range, 63.250.43.0/24.

Domain	IP	Registration Date
mypride[.]press	63.250.43[.]15 63.250.43[.]16	2023-02-27
warfareinsider[.]us	63.250.43[.]15 63.250.43[.]16	2023-07-05
besuchszweck[.]org	63.250.43[.]3	2023-02-24
hauynescherben[.]net	89.117.139[.]218 154.41.250[.]157	2023-07-05

Table 1: *mypride[.]press*, *warfareinsider[.]us*, and *besuchszweck[.]org* sharing the same subnet. While seemingly unrelated, *hauynescherben[.]net* was registered the same day as *warfareinsider[.]us*. (Source: Recorded Future)

21


TA-RU-2023-1205

Recorded Future® | www.recordedfuture.com



First-Stage Website	Second-Stage Website	Final Website
theearthangelconnection[.]com	jimjamfit[.]com	electionwatch[.]live
Unknown/Unavailable	buymeagradiant[.]com	mypride[.]press
lsfiry[.]gmailster[.]com	buymeagradiant[.]com	warfareinsider[.]us
zipplei[.]com risebedutt07[.]club	alfonrust[.]com, bookingyatri[.]com	besuchszweck[.]org
taigamebaisung[.]com	711ggr[.]com	grenzezank[.]com
only-best-kred119[.]buzz	fastnep[.]com	hauynescherben[.]net

Table 2: Sample path first- and second-stage websites used to conceal the final destination website used in Doppelgänger. Each of these websites is unique in the fact that they are an attempt to stand up original news outlets (Source: Recorded Future)

hauynescherben.net

2a02:4780:b:1041:0:1ec5:2b4c:4 

Lookup
Go To
Rescan
Add Verdict
Report

Submitted URL: <https://t.co/DPOZP8jbvs>
Effective URL: <https://hauynescherben.net/marktanalyse/deindustrialisierung-deutschlands-konkurrenzunfahige-strompreise-verdrangen-die-hei...>
Submission: On November 14 via manual (November 14th 2023, 9:21:54 pm UTC) from IT  — Scanned from GB 

Summary
HTTP 43
Redirects
Links 1
Behaviour
Indicators
Similar
DOM
Content
API
Verdicts

Page URL History

This captures the URL locations of the websites, including HTTP redirects and client-side redirects via JavaScript or Meta fields.

- <https://t.co/DPOZP8jbvs> Page URL
- <http://49g7l6.only-best-kred119.buzz/vpoumz> Page URL
- <http://fastnep.com/hauy6471691> HTTP 301
<https://fastnep.com/hauy6471691> Page URL
- <https://hauynescherben.net/marktanalyse/deindustrialisierung-deutschlands-konkurrenzunfahige-strompreise-verdrangen-die-heimische-industrie> Page URL



electionwatch.live

2a02:4780:b:730:0:3a37:5446:3 

Lookup
Go To
Rescan
Add Verdict
Report

Submitted URL: <https://t.co/cXLo9wgibm>

Effective URL: <https://electionwatch.live/futile-efforts>

Submission: On November 13 via manual (November 13th 2023, 12:47:19 am UTC) from IT  — Scanned from GB 

Summary
HTTP 27
Redirects
Links 2
Behaviour
Indicators
Similar
DOM
Content
API
Verdicts

Page URL History

This captures the URL locations of the websites, including HTTP redirects and client-side redirects via JavaScript or Meta fields.

- <https://t.co/cXLo9wgibm> Page URL
- <http://914uef.theearthangelconnection.com/2phzpw> Page URL
- <http://jiajamfit.com/elec8093802> HTTP 301
<https://jiajamfit.com/elec8093802> Page URL
- <https://electionwatch.live/futile-efforts> Page URL

Figures 29 and 30: Examples of full first- and second-stage redirects from social media to Häüyne Scherben and Election Watch. Insikt Group observed this pattern across all sources we attribute to Doppelgänger tracked in this report. (Source: [URLscan.io](https://urlscan.io) [1])

The second-stage websites utilized obfuscated JavaScript to send a GET request to another domain likely controlled by Doppelgänger, *ggspace[.]space*. When deobfuscated, the JavaScript reveals that the second-state domains send a request to *ggspace[.]space* likely using a campaign ID, as shown in **Figure 31**. The payload retrieves configuration information from the visitor's browser `localStorage` object. The following JavaScript crafts a new request containing tracking information (including the referrer ID, timestamp, and landing URL) to redirect the visitor to the final Doppelgänger domain.

```
(function() {  
  var name = '_ZTZrSwTJM1b1WD75';  
  if (!window._ZTZrSwTJM1b1WD75) {  
    window._ZTZrSwTJM1b1WD75 = {  
      unique: false,  
      ttl: 86400,  
      R_PATH: 'https://ggospace.space/UA-09-11_unian_-2',  
    };  
  }  
  const _9Nb953GKm5DpkF1k = localStorage.getItem('config');  
  if (typeof _9Nb953GKm5DpkF1k !== 'undefined' && _9Nb953GKm5DpkF1k !== null) {  
    var _N8MjDPxdMqDPQDYt = JSON.parse(_9Nb953GKm5DpkF1k);  
    var _RbVC8hfpTCMrWz6y = Math.round(+new Date()/1000);  
    if (_N8MjDPxdMqDPQDYt.created_at + window._ZTZrSwTJM1b1WD75.ttl <  
_RbVC8hfpTCMrWz6y) {  
      localStorage.removeItem('subId');  
      localStorage.removeItem('token');  
      localStorage.removeItem('config');  
    }  
  }  
}
```

Figure 31: Decoded JavaScript payload (Source: Recorded Future)

By analyzing JavaScript payloads found on other second-stage websites, we were able to identify campaign IDs using the following **Country_DD-MM_Target** format:

```
FR-14-10_lepoint  
FR-18-10_leparisien  
UA-17-10_unian_-2  
US-19-10_mypride  
US-19-10_warfareinsider  
DE-31-10_grenzezank  
DE-04-11_besuchszwec  
UA-07-11_rbk  
US-08-11_fox-news  
UA-09-11_unian_-2  
UA-10-11_rbk_-2  
US-11-11_electionwatch
```

Figure 32: Campaign IDs identified across second-stage websites (Source: Recorded Future)

Use of Keitaro TDS as Additional Doppelgänger Links

While information about *ggspace[.]space* remains sparse, we identified a login page at *ggspace[.]space/admin* (**Figure 33**). Pages with [identical login forms](#) [1, 2, 3, 4, 5] have been flagged as login pages for Keitaro Traffic Distribution System (TDS, *keitaro[.]io*), an analytics platform [previously reported](#) by Qurium as being used to analyze traffic to Doppelgänger assets in order to assess overall campaign performance and effectiveness.

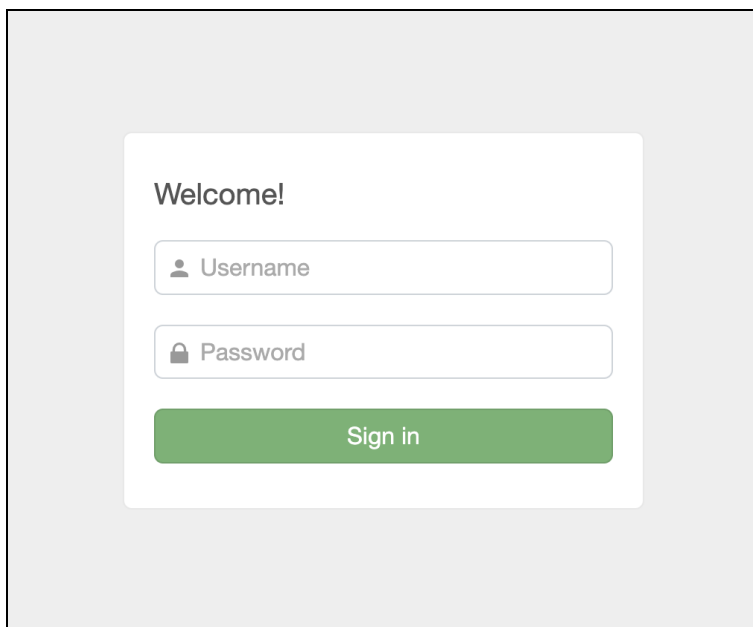


Figure 33: Keitaro TDS admin panel used by Doppelgänger (Source: [URLScan.io](https://urlscan.io))

Outlook

Doppelgänger exemplifies the enduring, scalable, and adaptable nature of Russian [information warfare](#), demonstrating strategic patience aimed at gradually shifting public opinion and behavior. As detailed in this report, Doppelgänger has demonstrated flexibility, adaptability, and an evolution in its tactics, such as its increased use of first- and second-stage websites, creating original but inauthentic news organizations, and likely using generative AI to produce influence content. Doppelgänger's evolving tactics suggest that the network is willing to invest in extra measures to evade detection and circumvent countermeasures, thereby making it more difficult for researchers and defenders to identify and disrupt malign influence activity. Doppelgänger will likely explore additional innovative tactics to further evade detection while trying to increase organic engagement with its content.

The indicators in this report provide technology companies, social media firms, and other researchers an opportunity to review current infrastructure and employ additional countermeasures to mitigate the effects of state-sponsored malign influence. The following list provides recommendations and strategies for continued mitigation and monitoring:

- This report, along with coverage from other research organizations and news agencies, serves as a tool to educate the public on Doppelgänger and provides a source to bolster public media literacy that is helpful for recognizing disinformation and effective prebunking. Periodically, [cautious bystanders](#) and commentary from [independent researchers](#) called into question the authenticity of the domains and corresponding content as we were tracking Doppelgänger, a very likely successful outcome associated with heightened online and media literacy, fact-checking skills, and prebunking tactics.
- Administrators of domains should continue to strengthen their defenses against cyberattacks, such as account hijacking, that threat actors can use to spread malign influence narratives and promote inauthentic news outlets hidden behind unrelated domains.
- We recommend that the counter-malign influence research community — including cybersecurity and threat intelligence firms, fact-checking organizations, journalists and media, research firms, independent researchers, and the public sector — continue cooperating and collaborating on monitoring, exposing, and countering Doppelgänger.
- Media organizations should also actively conduct brand monitoring to detect potential brand abuse from typosquatting domains, unauthorized use of organization logotype, and organization impersonation as well as journalist impersonation on social media and other open sources.

Appendix A: IOCs

Stage 1 Domains

Domain	IP	Owned By
rating-cred122[.]buzz	94.228.162[.]92	Aeza Group LLC
kbbet1[.]life	94.228.162[.]206	Aeza Group LLC
risebedutt07[.]club	94.142.138[.]17	Shelter LLC
taigamebaisung[.]com	94.142.138[.]17	Shelter LLC
arviewtv[.]org	94.142.138[.]17	Shelter LLC
gmailster[.]com	94.142.138[.]17	Shelter LLC
ger4098764793ggwhit3[.]online	45.91.8[.]61	SprintHost.RU LLC
ukgraphiclab[.]co[.]uk	45.91.8[.]61	SprintHost.RU LLC
norfolkcustomconcrete[.]com	45.91.8[.]61	SprintHost.RU LLC
karritech[.]co[.]uk	45.91.8[.]61	SprintHost.RU LLC
gardeningflair[.]com	45.91.8[.]61	SprintHost.RU LLC
yellowbarrels[.]co[.]uk	45.91.8[.]61	SprintHost.RU LLC
incawonders[.]com	185.46.46[.]122	YeezyHost
speaiker[.]com	185.46.46[.]122	YeezyHost
fl-studio-mobile-apk[.]online	185.46.46[.]122	YeezyHost
cypressnewsgh[.]online	185.46.46[.]122	YeezyHost
se5pro[.]co[.]uk	185.46.46[.]122	YeezyHost
abtbatteries[.]com	185.46.46[.]122	YeezyHost
decalworx[.]co[.]uk	185.46.46[.]122	YeezyHost
whatahotnews[.]com	185.251.91[.]91	SprintHost.RU LLC
pankajnakhat[.]com	185.251.91[.]91	SprintHost.RU LLC
ppplown[.]com	185.251.91[.]91	SprintHost.RU LLC
penisbreakfast[.]com	185.251.91[.]91	SprintHost.RU LLC
pwscontrols[.]com	185.251.91[.]91	SprintHost.RU LLC
whencontact[.]com	185.251.91[.]91	SprintHost.RU LLC
renderny[.]com	185.251.91[.]91	SprintHost.RU LLC
yassirjamal[.]com	185.251.91[.]91	SprintHost.RU LLC
chickenhug[.]com	185.251.89[.]255	SprintHost.RU LLC

frisurenmarkt[.]com	185.251.89[.]255	SprintHost.RU LLC
turn[.]click	185.251.89[.]255	SprintHost.RU LLC
customautobodyaz[.]com	185.251.89[.]255	SprintHost.RU LLC
leidatova[.]com	185.251.89[.]255	SprintHost.RU LLC

Table 3: First-stage websites observed in Insikt Group's Doppelgänger investigation (Source: Recorded Future)

Stage 2 Domains

Domain	IP	Final Destination Example
711ggr[.]com	206.71.148[.]217	https://grenzezank[.]com/spaltung-in-der-nato/
alfonrust[.]com	206.71.148[.]217	https://besuchszweck[.]org/tod-fur-migranten
buymeagradient[.]com	206.71.148[.]217	https://warfareinsider[.]us/us-troops-could-be-deployed-in-israel-if-situation-is-out-of-control/
freemit[.]com	206.71.148[.]217	https://www.lepoint[.]foo/politique/Beaucoup-de-bruit-et-puis-rien-07-10-2023-2528358_20.php
govreadyq[.]com	206.71.148[.]217	https://www.unian[.]pm/politics/ukraintsev-predupredili-o-l-ednikovom-periode.php
incredipoll[.]com	206.71.148[.]217	https://www.rbk[.]media/rus/news/zelenskomu-nuzhna-oc-herednaja-mjasorubka.php
maddiecrum[.]com	206.71.148[.]217	https://www.unian[.]pm/politics/v-stile-mafii.php
matiasbenavides[.]com	206.71.148[.]217	https://www.rbk[.]media/rus/news/novyj-sposob-ograbit-s-voih.php

Table 4: Second-stage websites observed in Insikt Group's Doppelgänger investigation (Source: Recorded Future)

Stage 3 Inauthentic News Outlets and Impersonation Domains

Domain	Domain
electionwatch[.]live	hauynescherben[.]net
mypride[.]press	rbk[.]media
warfareinsider[.]us	unian[.]pm
besuchszweck[.]org	obozrevatel[.]ltd
grenzezank[.]com	

Table 5: Final redirected domains tracked in Insikt Group's Doppelgänger investigation, targeting Ukrainian, US, and German audiences (Source: Recorded Future)

Additional Stage 3 Domains Identified During Investigation

Domain	Domain
50statesoflie[.]com	levinaigre[.]net
acrosstheline[.]press	liesofwallstreet[.]com
cropmarketchronicles[.]us	meisterurian[.]io
derbaterischelowe[.]info	news.walla.com[.]co
derleitstern[.]com	news.walla[.]re
eurobrics[.]de	notrepays[.]today
fox-news[.]in	observateurcontinental[.]fr
holylandherald[.]com	rrn[.]media
lavirgule[.]news	spiegel[.]ltd
la-croix[.]cam	theliberal[.]in
lebelligerant[.]com	tribunalukraine[.]info
leparisien[.]pm	washingtonpost[.]pm
lepoint[.]foo	welt[.]ltd

Table 6: *Insikt Group also identified additional domains impersonating Western news organizations and original inauthentic news websites over the course of our research. Several of these domains were reported in open sources as being linked to Doppelgänger. [EU DisinfoLab](#) previously attributed the domain [observateurcontinental\[.\]fr](#) to InfoRos, a news outlet linked to Russian military intelligence (GRU). (Source: Recorded Future)*

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com