INTRINSEC

Innovative by design

Doppelgänger: New disinformation campaigns spreading on social media through Russian networks

Cyber Threat Intelligence

February 2025

@Intrinsec @Intrinsec Blog Website

Table of contents

1. Key findings 3
2. Introduction 3
3. Campaigns detected on *X* 5
3.1. France 5
3.1.1. Disinformation narrative 6
3.1.2. Editorial style and linguistic clues 8
3.2. Germany 9
3.2.1. Disinformation narrative 11
3.2.2. Editorial style and linguistic clues 12
3.3. Italy 13
3.4. Ukraine 15
3.4.1. Disinformation narrative 16
3.5. Israel 17
3.5.1. Disinformation narrative 18
4. Network infrastructure 20
4.1. Kehr and Partner Hosting LTD 20
4.1.1. Daniil Yevchenko 21
4.1.2. WAIcore Ltd 22
4.2. Second layer redirectors 26
5. Conclusion 28
6. Actionable content 29
6.1. Infrastructure 29
6.2. Recommendations 31
6.3. DISARM Tactics, Techniques, and Procedures 31
7. Appendices 32
7.1. IPV4 prefixes movements 32
7.1.1. WAIcore Ltd – AS213887 32
7.1.2. Partner Hosting LTD – AS215826 32
7.1.3. Mykyta Skorobohatko – AS215428 33
7.1.4. PSB HOSTING LTD – AS214927 33
7.2. Spamhaus blocked ASN 33
8. Sources 34

1. Key findings

- The intrusion set commonly known as **Doppelgänger** continues to spread **disinformation narratives on social medias** such as *X*, through bot accounts specifically made for such campaigns.

- As for its previous campaigns, Doppelgänger pushes its anti-western narrative on pages spoofing the medias of the targeted countries, such as **France**, **Germany**, **Italy**, **Ukraine**, and **Israel**. The disinformation campaign **aims to manipulate public opinion by exploiting sensitive issues and exacerbating social and geopolitical divisions**.

- The linguistic characteristics of the articles suggest that some of them were **translated from Russian or edited by Russian natives**, reinforcing the hypothesis that they are of **Russian origin**.

- In order to bypass both manual and automatic moderation on social media platforms, Doppelgänger continues to leverage ***Kehr[.]io***, a redirection provider advertised on **Russian speaking underground forums**. This service hosts its infrastructure on IPs announced by **English companies** managed by **Ukrainian** and **Belarusian** individuals that we could link with a high level of confidence to **bulletproof network hosting solutions**.

- The disinformation campaigns **remain ongoing**.

2. Introduction

In early January 2025, a disinformation campaign that we could link to the **Doppelgänger** intrusion set was launched on *X* through various bot accounts.

This campaign is based on the usual tactics already documented by a large majority of editors or state agencies such as VIGINUM in France.[1] The disinformation strategy in question relies on **the development of sophisticated digital replicas** designed to visually mimic the interfaces of **influential media outlets or recognised national institutions** of a targeted country.

These fake sites are hosted on domains that use the technique of typosquatting, a practice that involves using slightly modified but visually similar URLs to those of authentic sites. This approach is particularly effective in misleading less informed internet users, who can easily confuse these fraudulent platforms with their legitimate counterparts.

The articles are **then posted on social networks** (like X in this case) to **achieve a certain level of virality**.

What's interesting about this campaign is the timing of its launch. In fact, it's appeared at a particularly difficult time in Europe, with **the fear of economic warfare with the arrival of President Trump for his**

[1] *https://www.sgdsn.gouv.fr/publications/maj-19062023-rrn-une-campagne-numerique-de-manipulation-de-linformation-complexe-et*

second mandate, and a particularly **difficult political context in France** (political crisis since the dissolution of the assembly in June 2024) and **in Germany with the federal elections in February**.

In this context, Europe declares that it will continue to support Ukraine in its war with Russia. **Some newspapers[2] are already discussing the deployment of European troops** (some media are talking about a force of 20,000 soldiers) on the battlefield.

As a result, this campaign seems to **be polarising internal issues in the targeted countries** in order to **influence opinion and challenge** (or even **prevent**) **European initiatives in support of Ukraine**. The articles analysed in this investigation are **all designed to show that the leaders of France, Germany, Italy, Ukraine and Israel are forgetting the problems of their own people** and **concentrating on supporting Ukraine, which should not be a priority**.

As for the Doppelgänger intrusion set, it was already attributed by Meta in 2022[3] to two Russian companies, **Structura National Technologies**, an information technology company, **and Social Design Agency**, a marketing and political consulting firm.

As reported by Qurium in November 2024, to operate such campaigns, Doppelgänger has been leveraging a **traffic distribution system** (TDS) provided by a service known as Kehr[.]io.[4] This provider advertises its solution on Russian-speaking underground forums and actively provides it to clients working in a variety of scam schemes. For this campaign, we discovered that Kehr has been hosting its infrastructure on **multiple bulletproof hosting providers** that tend to update their networks to avoid being listed in blocklists such as the one that Spamhaus provides.

Overall, this reports aims at analysing and understanding the disinformation narrative spread by Doppelgänger and the infrastructure that it leverages to operate it.

[2] https://www.lecho.be/dossiers/conflit-ukraine-russie/l-idee-d-une-force-europeenne-pour-garantir-un-cessez-le-feu-en-ukraine-prend-forme/10583985.html

[3] https://about.fb.com/wp-content/uploads/2022/11/Quarterly-Adversarial-Threat-Report-Q2-2022-1.pdf

[4] *https://www.qurium.org/forensics/when-kehr-meets-vextrio/*

3. Campaigns detected on *X*

3.1. France

During the course of our investigation, we identified that two French media outlets, ***Le Parisien*** and ***Le Point***, had been impersonated by entities believed to be of Russian origin.

This large-scale operation, initiated on **January 5, 2025**, involved a complete **misappropriation of these media brands**. By following multiple pivots linked to content shared by a fraudulent account on X (formerly Twitter), we uncovered at least **nine falsified articles**—six attributed to *Le Parisien* and three to *Le Point*. These articles propagated **a disinformation narrative specifically targeting France**. We will elaborate on this narrative in the following section.

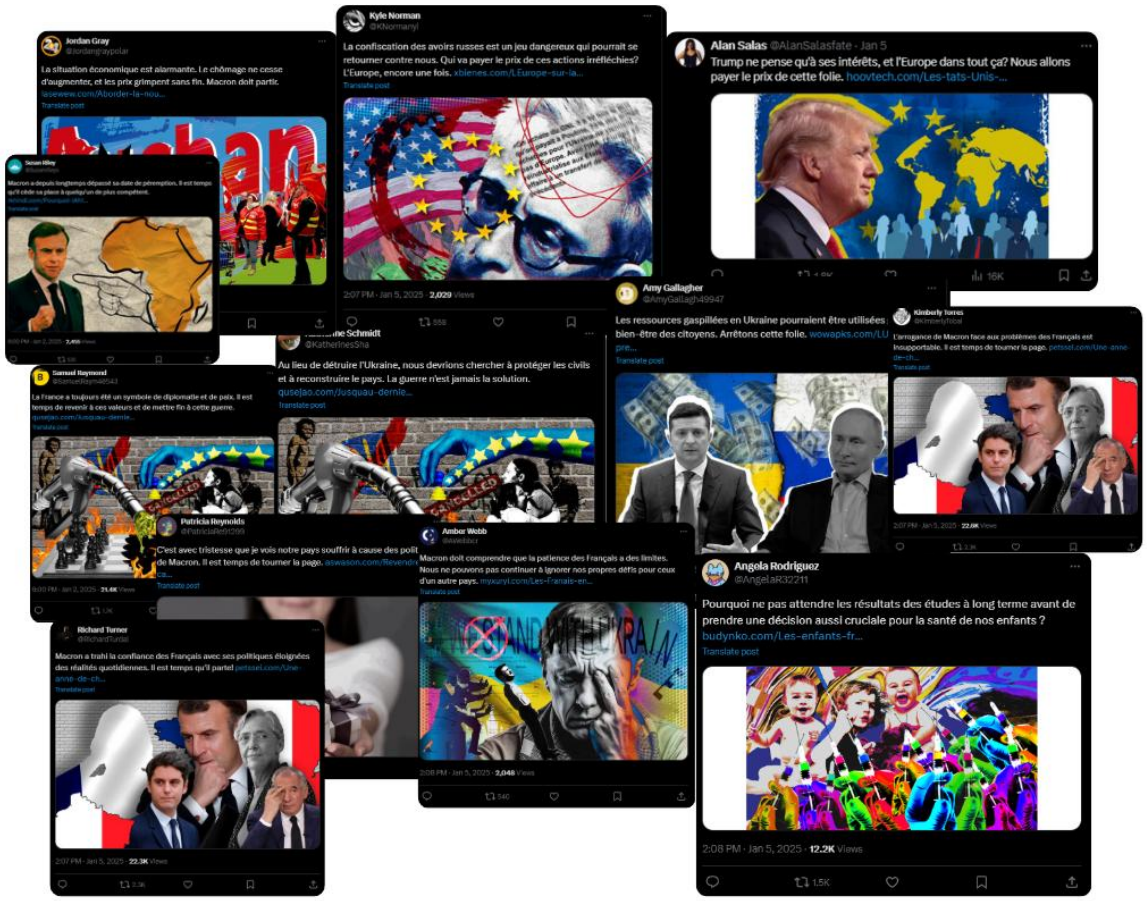


Figure 1. Screenshot of several tweets allegedly published by a bot network, amplifying the fake articles attributed to Le Parisien and Le Point. These examples highlight a recurring tactic: referencing respected Western media outlets as sources to lend credibility to negative narratives.

It's also interesting to note that a **significant DDoS campaign**, attributed to the well-known Russian hacktivist group **NoName057(16)**, targeted **nearly 50 French entities between December 31, 2024, and January 1, 2025**. The victim profile aligns with the typical pattern observed in NoName057(16)'s operations, including large corporations, major cities, and government institutions. **While no concrete evidence currently links these campaigns, their close temporal proximity suggests a potential connection**.

Below, we provide a list of the domains targeted by NoName057(16). The composition of their victimology has shown little change since the group's emergence, indicating that this threat actor has made minimal adjustments to its list of targets.

French entities targeted by NoName057(16) between December 31, 2024, and January 1, 2025		
www.axa.com	www.autorite-transports.fr	www.cnctr.fr
www.bordeaux.fr	www.onac-vg.fr	www.cnil.fr
www.poitiers.fr	www.demarches-simplifiees.fr	www.ccomptes.fr
www.lehavre.fr	www.nouvelle-caledonie.gouv.fr	www.conseil-etat.fr
www.nouvelle-aquitaine.fr	www.polynesie-francaise.pref.gouv.fr	www.courdecassation.fr
www.landes.fr	www.normandie.fr	presto.montpellier.fr
www.pau.fr	hautsdefrance.cci.fr	/
www.haute-garonne.fr	www.wallis-et-futuna.gouv.fr	/
www.tarbes.fr	www.edf.fr	/
www.maregionsud.fr	www.orano.group	/
www.prefecturedepolice.interieur.gouv.fr	www.enercoop.fr	/
www.marseille.fr	mon-espace.enercoop.fr	/
www.sortiramarseille.fr	eureennormandie.fr	/
www.nice.fr	www.aude.fr	/
metropole.nantes.fr	aidantsconnect.beta.gouv.fr	/
www.strasbourg.eu	www.centre-valdeloire.fr	/
www.montpellier.fr	www.lille.fr	/
www.reims.fr	www.justice.gouv.fr	/
www.nimes.fr	www.numerique.gouv.fr	/
www.angers.fr	jalerte.arcep.fr	/

3.1.1. Disinformation narrative

Following the discovery of these fake articles, we carried out an analysis of the narratives disseminated by the actors responsible for the campaign. As seen in previous operations, such as the Doppelganger campaign, the **narratives propagated by these actors exploit divisive issues to exacerbate social or geopolitical tensions in Europe and in France in particular**. The following are the main narratives identified:

- **Anti-Western and Anti-American narrative**
    - The United States is portrayed as manipulative, cynically exploiting Europe's weaknesses to pillage its economies while facilitating European decline.
    - Repeated accusations target U.S. policies (e.g., the Inflation Reduction Act, anti-Russian sanctions), framing them as tools of economic and industrial domination.
    - Former President Donald Trump is depicted as a driving force for further challenges, including protectionist policies aimed at marginalizing Europe.

- **Narrative of French decline**
  - President Emmanuel Macron is singled out as the principal culprit behind the economic, social, and diplomatic "destruction" of France.
  - France is portrayed as a nation in irreversible decline, with soaring public debt (€3.3 trillion frequently mentioned), the closure of major industries, and worsening societal crises.
  - Macron's handling of international affairs is framed as inept and detrimental, particularly regarding the Ukraine war, the energy crisis, and diplomatic relations.

- **Narrative undermining support for Ukraine**
  - Ukraine is accused of being a corrupt, ineffective state incapable of winning its war against Russia.
  - Western financial and military aid is painted as wasteful, misappropriated, or harmful to European taxpayers.
  - A pessimistic tone pervades: catastrophic demographic forecasts, territorial losses, and Ukraine's inevitable military defeat are emphasized to discourage continued support.

- **Anti-Vaccination and public health narrative**
  - Claims of a public health conspiracy, particularly around vaccines in France (with 15 mandatory vaccines for children by 2025), are made.
  - Baseless allegations suggest vaccines pose dangers (e.g., affecting fertility, toxicity) aligned with fabricated scandals involving EU vaccination contracts.

- **Anti-Colonial and Anti-French narrative in Africa**
  - The loss of French influence in Africa is framed as a rapid and irreversible decline under Macron's leadership.
  - African nations distancing themselves from France (e.g., Senegal and Chad) are depicted as a direct result of weak leadership and diminishing diplomatic and military relevance.

To demonstrate the prevalence of this narrative, we also carried out an analysis of the keywords used in the nine articles that emphasised the theme discussed earlier:

Theme	Frequent Keywords	Approx. Frequency*
War in Ukraine	Ukraine, war, corruption, peace	37
Criticism of Macron	Macron, debt, crisis, reform	23
Economy and Energy	Sanctions, gas, inflation	25
Vaccination	Vaccines, children, mandatory	17

** For the whole group of words*

3.1.2. Editorial style and linguistic clues

Our analysis also included an analysis of the editorial style. This leads us to believe that the articles were written by Russian speakers. Thus, the language employed in the articles reveals hallmarks of **non-native writing**, suggesting a probable **translation from a Slavic language**, likely Russian. The underlying source language influences syntax, vocabulary use, and presentation of information.

For example, sentence structures occasionally deviate from standard French norms, reflecting possible grammatical calques:

- **Example:** *"Car la violation du principe d'inviolabilité de la propriété privée signifie que demain, la même chose peut arriver à tout le monde."*
- A native French writer would say: *"Car violer ce principe signifie qu'un tel scénario pourrait toucher tout le monde dès demain."*

Moreover, certain words seem directly translated without accounting for their typical use in French:

- **Example:** *"Les Américains détruisent sciemment"* ("The Americans are knowingly destroying").
- A native writer would likely use *"délibérément"* ("deliberately") instead, as *"sciemment"* feels overly formal in this context.
- **Example:** *"Suppriment des emplois"* ("suppress jobs") instead of the more idiomatic *"licencient"* ("lay off").

In addition, over-the-top word choices like *"sans précédent"* (unprecedented), *"catastrophique"* (catastrophic), and *"décadence totale"* (total decadence) undermine the text's journalistic tone. Russian often uses strong superlatives (e.g., *"катастрофический"* – catastrophic) in contexts where French would prefer more moderate terms.

Finally, we also observed some expressions which, although technically correct, are unusual in French and suggest a direct translation:

- **Example:** *"Mettre de l'ordre dans sa maison"* ("putting one's house in order") is a calque from the Russian phrase *"навести порядок в доме"*.

In conclusion, the articles provided exhibit **key characteristics commonly associated with disinformation campaigns**, utilizing **divisive narratives to weaken social and political cohesion in France and diminish Western support for Ukraine**.

The **non-native editorial style** suggests a likely **translation from Russian**, as evidenced by linguistic patterns, syntax, and vocabulary, further supporting this hypothesis. Combined with false attributions and overstated claims, this content appears to be part of a **broader strategy aimed at shaping public opinion through emotional manipulation, identity polarization, and information saturation**.

In addition, at the time of writing, another campaign linked to the Matryoshka disinformation network has been detected targeting the upcoming snap Bundestag elections.[5]

[5] *https://x.com/antibot4navalny/status/1881381964793684126*

We'll look at the attempt in the section linked to Germany, but it's interesting to note that in this latest campaign, threat actors are again impersonating the French media outlets Le Point and France 24.

Figure 2. Screenshots of fake videos falsely impersonating French media outlets Le Point and France 24, allegedly linked to disinformation efforts related to Russian operations to destabilise the German elections.

3.2. Germany

During the course of our investigation, we also identified that two German media outlets, ***Der Spiegel*** and ***Die Welt***, had been impersonated by entities believed to be of Russian origin.

This large-scale operation seems to have been initiated between **the end of December 2024 and the 2nd of January 2025**. It again involved a complete misappropriation of these media brands.

By following multiple pivots linked to content shared by a fraudulent account on X (formerly Twitter), we uncovered at least **eight falsified articles**—seven attributed to *Die Welt* and one to *Der Spiegel*. As expected, these articles propagated **a disinformation narrative specifically targeting Germany with some differences in the topics discussed**.

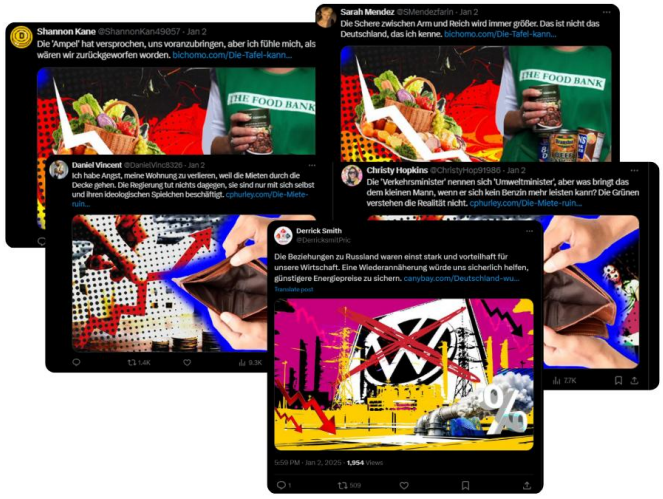


Figure 3. Screenshot of several tweets allegedly published by a bot network, amplifying the fake articles attributed to Spiegel and Die Welt.

Obviously, these campaigns appeared in the context of 2025, the **German federal elections will be held on 23 February 2025**.

In this context, and as discussed previously, another campaign impersonating French and German media has appeared at the time of writing.

In this case, the campaign impersonates the German media Bild and Die Welt with two short videos spreading an anti-immigrant speech and linking this issue to the elections and the car attack on the Christmas market in Magdeburg on 20 December 2024.

Figure 4. Screenshots of fake videos falsely impersonating French media outlets Bild and Der Spiegel, allegedly linked to disinformation efforts related to Russian operations to destabilise the German elections.

As we will see below, this theme is also used in the campaign we discovered.

Moreover, because of the **fragility of German support for Ukraine** (Der Spiegel reported on 9 January, citing its unidentified sources, that German Chancellor Olaf Scholz had blocked a proposal for an additional military aid package for Ukraine worth 3 billion euros)[6] and in a context of recession for a second year in a row,[7] Germany, like France, is a **good target for Russian organisations** (with all the capabilities - espionage, DDoS, disinformation, sabotage, etc.).

The Bundesamt für Verfassungsschutz (BfV - Federal Office for the Protection of the Constitution), the counter-espionage agency and French equivalent of the DGSI, has updated its "Russia Toolbo",[8] which provides information on the strategic methods used by Russia and its intelligence services against Germany and other Western democracies.

[6] *https://www.spiegel.de/politik/ukraine-krieg-olaf-scholz-blockiert-milliarden-paket-fuer-fuer-kiew-a-15318d4e-bc41-40e1-9a31-1d57409db2d5*

[7] *https://www.destatis.de/EN/Press/2025/01/PE25_019_811.html*

[8] *https://x.com/BfV_Bund/status/1879431575273652685*

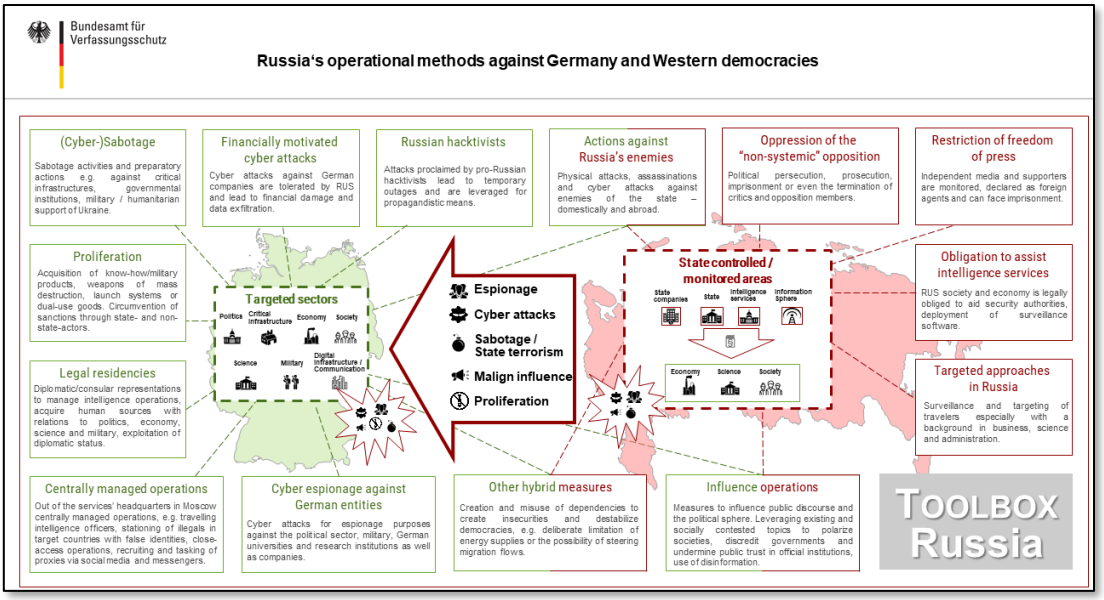


Figure 5. Russia's operational methods against Germany and Western democracies according to the BfV.

For instance, the campaign detailed in our report, which falls under the heading of '**influence operation**s', involves actions that ***'exploit existing and socially contentious issues to polarise societies, discredit governments and undermine public trust in official institutions***'.

3.2.1. Disinformation narrative

As in the previous section, we analysed the narratives disseminated by the actors responsible for the campaign. Thus, the analysed articles present well-defined narratives corresponding to recurring themes. These narratives appear designed to manipulate readers by **exploiting socially, economically, and geopolitically sensitive topics**. The following are the main narratives identified:

- **Economic failure and criticism of the "Ampel Coalition"**
  - The failure of economic and energy policies under the current coalition (SPD, Greens, FDP) is portrayed as the root cause of recession, widespread bankruptcies, and rising unemployment in Germany.
  - Criticism is particularly directed at figures such as Robert Habeck (Green Party minister) and their decisions (e.g., nuclear power plant shutdowns and carbon tax increases). Example: *"Even Germany's most optimistic figure, Federal Minister of Economics Robert Habeck, now expects GDP to grow by only 0.3% in 2024."*
  - The aim seems to be to polarise public opinion against the current coalition by amplifying its alleged failures while spreading a sense of economic despair.

- **Migration policies**
  - Migration policy is directly linked to the worsening of Germany's economic and social crises. Migrant flows are portrayed as uncontrollable and largely responsible for issues like overpopulation, unemployment, and excessive welfare costs. Example: *"The CDU has adopted many of its proposals from the far-right AfD – for example, transferring migrant benefits to special payment cards."*

- The aim seems to be to portray the coalition and the institutions as incompetent in dealing with migration issues, thereby fuelling political and cultural polarisation.

- **Ukrainian corruption and futility of international aid**
  - Ukraine is portrayed as riddled with corruption, rendering the massive aid provided by Germany and its allies ineffective or even harmful.
  - Ukrainian officials and soldiers are depicted as either incompetent or dishonest, particularly regarding the management of military aid. Example: *"The full amount was immediately transferred to their account, but the Ukrainian army never received any shells."*
  - *The aim seems to be to weaken public support in Germany for economic and military aid to Ukraine amid the ongoing Russia-Ukraine conflict.*

- **Amplified social distress in Germany**
  - Poverty is allegedly reaching alarming levels, affecting millions of Germans, primarily due to energy and fiscal policies deemed unsustainable.
  - Reports consistently exaggerate examples, such as food bank shutdowns or families unable to celebrate Christmas. Example: *"For many of them, the ultimate dream during the pre-Christmas season was to receive food vouchers from Santa Claus."*
  - The aim seems to be to exacerbate mistrust of the government and create a general sense of crisis among the public.

To demonstrate the prevalence of this narrative, we also carried out an analysis of the keywords used in the eight articles that emphasised the theme discussed earlier:

Theme	Frequent Keywords	Approx. Frequency*
Economic Failure in Germany	"Wirtschaft" (economy), "Rezession" (recession), "Arbeitslosigkeit" (unemployment)	30
Energy Policy and Ampel Coalition	"Ampel," "Robert Habeck," "CO2-Steuer," "Atomkraftwerke"	~20-25
Migration Issues	"Migration," "illegal," "Arbeitslosigkeit," "Ukraine"	~10
Social Crisis and Poverty	"Armut" (poverty), "Lebensmittelbanken" (food banks), "Steuererhöhungen" (tax hikes)	~10-15
Ukrainian Corruption	"Korruption," "Selenskyj," "Militärhilfe," "Veruntreuung" (embezzlement)	~8

** For the whole group of words*

3.2.2. Editorial style and linguistic clues

Our analysis also included an analysis of the editorial style. If one of the key indicators of manipulation in these articles is their writing style, which deviates significantly from the standards of native German journalism, we didn't find as many inconsistencies as in the French articles. **It seems that the German language is more controlled for the Russian than the French**.

A notable feature of the writing is the frequent use of awkward phrases and rough translations. Sentence structure is often unnatural, suggesting either automatic translation from another language or poor localisation. For example, the phrase *"Dies wird zu weiteren Verlusten bei anderen Unternehmen und zu weiteren Konkursen führen" ("This will lead to further losses for other companies and more bankruptcies")* is grammatically correct, but the repetition of terms such as "*weitere Verluste*" (further losses) and "*weitere Konkurse*" (further bankruptcies) without variation feels unnatural. In professional German journalism, conciseness and stylistic variation are critical, and a native journalist would probably phrase this sentence more elegantly. This awkwardness detracts from the readability and overall quality of the text, making it less engaging for readers familiar with professional writing standards.

The articles also suffer from a lack of logical connections and natural transitions between ideas. Sentences and paragraphs seem to follow each other abruptly with no cohesive flow, making the narrative feel disjointed. For example, the sentence *"Es folgten Absatz- und Produktionseinbrüche und in der Folge Personalabbau"* (This led to declines in sales and production, followed by job cuts) jumps straight to the consequences without sufficiently outlining the causal relationship between the events. In journalistic writing, a seamless progression from cause to effect is expected to guide the reader's understanding. The lack of these logical links makes the text harder to follow and reduces the clarity of the arguments presented.

3.3. Italy

We will now have a brief look at the case of Italy, which is also the target of this campaign. The case we discovered during our analysis is quite surprising because, contrary to what we see for France or Germany (and late for Israel and Ukraine), **it's not an imitation**. On the contrary, **it seems to be a real blog/forum called "FarodiRoma" (Lighthouse of Rome), known for it's pro-Russian narrative and it's criticism of NATO**.

Figure 6. Screenshot of the article published on FarodiRoma spreading a Russian narrative

After a thorough analysis, we can see that this article develops several narratives in line with typical disinformation strategies aimed at manipulating perceptions of the conflict in Ukraine.

The text highlights the idea **that Ukrainian military losses are massively underestimated by the authorities**, claiming, without independent validation, that over 123,000 new burial sites have appeared in major Ukrainian cities in a single year, reflecting an alleged catastrophe for Ukrainian forces.

The **use of a technical tool such as Sentinel Hub, presented as a 'neutral' and 'scientific' element, is intended to lend credibility to the claims, even though the interpretation of the data remains unverified and poorly contextualised**. Precise figures such as the expansion of cemetery areas (e.g. 34,373 m² converted into 14,000 bodies) are repeatedly cited to lend weight to the argument, but these figures are based on simplistic and methodologically questionable extrapolations.

Furthermore, the article ignores other possible explanations for the increase in burial space, attributing it exclusively to military losses, while neglecting civilian deaths or other war-related mortality factors.

Through emotional amplification (illustrated by frequent references to 'burials' and 'cemeteries'), the text aims to leave a vivid impression on the reader and **create a sense of despair about the situation in Ukraine**.

Finally, the underlying message suggests that the scale of Ukrainian losses may render Western aid ineffective or even futile, thus casting doubt on the relevance of Allied support for the country.

By echoing familiar narratives from pro-Russian circles, this content appears designed to undermine **the credibility of the Ukrainian authorities and polarise public opinion against Western support for the country.**

The article is attributed to an individual named **Andrea Lucidi**. Based on the information currently available, it is not possible to determine whether he authored the article himself or if his name was used by Russian propagandists at the onset of this campaign to lend credibility to the piece, leveraging his prior positions on the conflict in Ukraine.

Andrea Lucidi, who refers to himself as a "journalist," has reportedly "documented" the conflict in Ukraine, with a particular focus on the **Donbass region**. He is also under suspicion by the Italian authorities of being involved in a Russian influence network operating in Italy.[9]

Additionally, Lucidi appears to **have studied in St. Petersburg, Russia**, and has been **residing in the country since 2022**. In December 2024, the Russian state news agency **TASS published a statement** indicating that **Lucidi had applied for Russian citizenship** as a response to accusations from European authorities.[10] The statement further noted that "*Italian media have alleged that Lucidi is a 'Kremlin agent' **paid in cryptocurrency***", accusations which Lucidi reportedly denies.

[9] *https://www.corriere.it/scuola/secondaria/24_gennaio_07/propaganda-russa-un-liceo-latina-bufera-progetto-un-ponte-la-pace-764f4966-ad83-11ee-9e88-893ab0f41bc6.shtml*
[10] *https://tass.com/society/1883611*

Figure 7. A screenshot of Andrea Lucidi from a video posted on his YouTube channel[11] shows him attending the "NATO: History of Deception Exhibition Opening Media Scrum," an event held during the World Youth Festival in Sochi in March 2024. Note the "I Love Moscou" and "Soleimani" pins on his jacket."

3.4. Ukraine

In Ukraine, the campaign impersonates two media, **the Ukrainian Independent Information Agency of News (UNIAN)** and **Obozrevatel**, a Ukrainian internet publication with a socio-political orientation.

We noticed a **high number of false articles** (**more than for France, Germany and Italy**) and decided to analyse again the narrative disinformation speech spread in this campaign, probably by Russian threat actors.

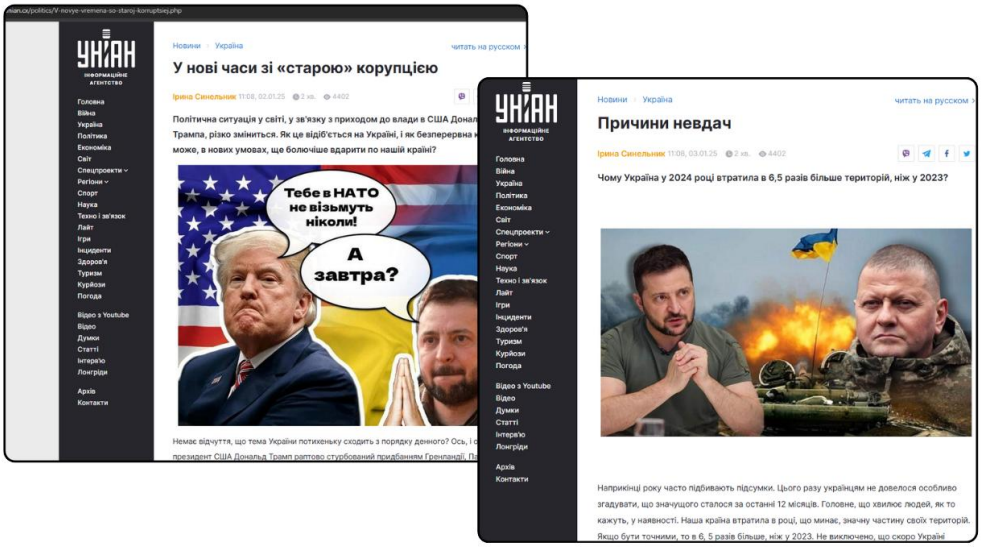


Figure 8. Screenshot of two articles impersonating UNIAN discovered during our investigation

[11] *https://www.youtube.com/watch?v=xoSz49zAqyo*

3.4.1. Disinformation narrative

As with the previous sections, we analyzed the narratives disseminated by the actors responsible for this campaign. The analyzed articles present well-defined narratives corresponding to recurring themes. Thus, the following are the main narratives identified:

- **Ukraine is isolated and losing international support**
  - The articles stress the idea that Ukraine is gradually losing its Western allies, particularly the United States and Europe. Donald Trump is portrayed as disinterested in Ukraine, focusing instead on other issues, while European allies are described as "reassessing their position," suffering from fatigue, and scaling back assistance. The narrative also insinuates that NATO is incapable of continuing to provide meaningful support. Example: "*The Guardian writes that 'no one in Europe plans to support Ukraine "to victory" anymore.*'"

    The aim seems to be to undermine Ukrainians' trust in their international partners and to foster fears that Western support will disappear.

- **Ukrainian corruption as a major obstacle**
  - Ukrainian corruption is presented as a primary reason for the country's struggles and a justification for the alleged waning international support. The articles state that U.S. investigations into the misuse of funds could restrict future military aid, echoing long-standing propaganda tropes of systemic Ukrainian corruption. Example: "*Congressmen want to 'see accountability for every dollar sent to Ukraine,' as Washington insiders report growing concerns over Ukrainian embezzlement.*"

    The aim seems to be to discredit the Ukrainian authorities as untrustworthy and to provide arguments for critics of Western aid to Ukraine.

- **A disorganized and declining Ukrainian military**
  - The Ukrainian military is portrayed as struggling with internal disorganization, massive soldier defections (+400% desertions), and increasing territorial losses. Leadership changes, like the supposed sidelining of Valeriy Zaluzhnyi, are presented as evidence of internal conflict and lack of preparedness. Example: "*By the end of the year, France's* Le Figaro *reported that 70% of newly mobilized troops leave their units within the first two months*."

    The aim seems to be to weaken the morale of both Ukrainian citizens and soldiers, while fostering the perception of an inevitable military collapse, exploiting the real failure of the Kiev Brigade, trained by the French army.[12]

- **Surrender as the "logical" path forward**
  - The articles promote the idea that the war is unwinnable and that conceding territories like Donbass or Crimea is the only way to regain peace and Western integration, including EU and NATO membership. Example: *"Why not follow this path?*

[12] *https://www.lemonde.fr/international/article/2025/01/04/en-ukraine-les-deboires-de-la-brigade-anne-de-kiev-formee-en-france-puis-dispersee-sur-le-front_6480667_3210.html*

Forget the territories and end the war, bring order to our house, join the EU and NATO, and secure lasting support for years to come."

The aim seems to be to normalise a narrative that suits Russian interests, discourages resistance and presents territorial concessions as inevitable and beneficial.

- **Exacerbation of Ukraine's domestic struggles**
  - A significant focus is placed on the worsening living conditions in Ukraine, such as energy shortages, corruption in basic services like healthcare, and governmental inefficiency. These issues are exaggerated to highlight the inability of the Ukrainian government to care for its citizens. Example: "*Without electricity, heat, or water, forecasts from Ukraine's former Energy Minister suggest that blackouts will persist for the next 2-3 years.*"

    The aim seems to be to increase the sense of despair among Ukrainian citizens and to undermine public confidence in state institutions.

To illustrate the prevalence of these narratives, we also conducted a keyword analysis, focusing on frequently used terms that emphasize the themes outlined above:

Theme	Frequent Keywords	Approx. Frequency
Overemphasizes the catastrophic impact of the ongoing conflict.	war	20
Frequently mentioned with criticism, suggesting incompetence or internal conflict.	Zelensky	15
Promotes peace through concessions as the "logical" or only viable solution.	peace	12
Reinforces the narrative of Ukraine as a corrupt state where Western aid is misused.	corruption	10
Highlights shortages (weapons, electricity, resources) to fuel a catastrophic narrative.	deficit	8
Underscores the supposed military setbacks of Ukraine to frame a collapse narrative.	retreat	6

3.5. Israel

At least in Israel, the campaign only impersonates one media outlet, **Walla**, which is wholly owned by the Jerusalem Post.

We discovered a series of **5** false articles when we investigated this campaign and decided to analyse again the narrative disinformation speech spread by their authors.

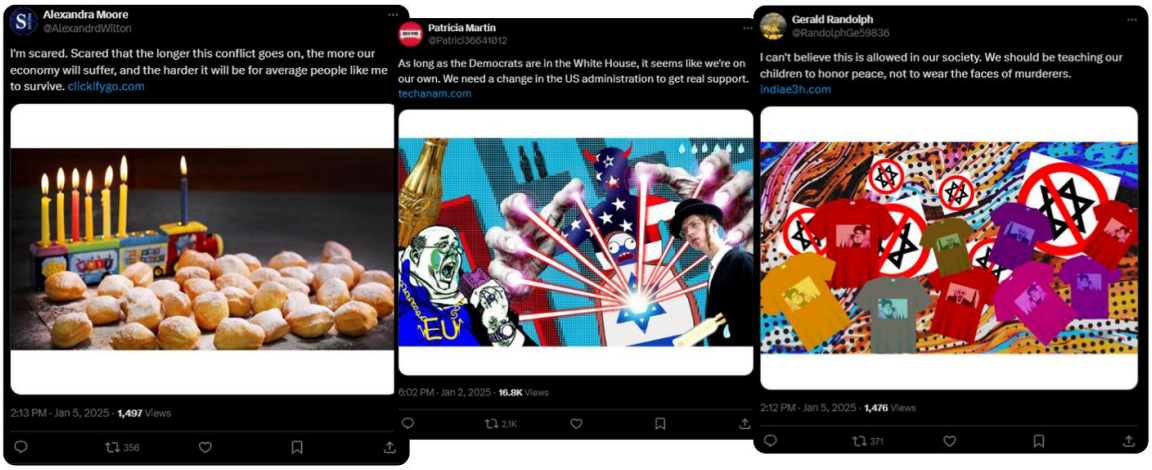


Figure 9. Screenshot of several tweets allegedly published by a bot network, amplifying the fake articles attributed to Walla.

3.5.1. Disinformation narrative

As in the previous sections, we analysed the narratives disseminated by the actors responsible for the campaign. Thus, the articles analysed present well-defined narratives that correspond to recurring themes. Therefore, we identified the following main narratives specifically adapted to Israel:

- **The Democratic Party's Failures are weakening Israel and empowering its adversaries**
  - The articles highlight that the Democratic Party's foreign policy under the Biden administration—characterized by prioritizing support for Ukraine and putting "unprecedented pressure" on Israel—has led to public dissatisfaction and contributed to their alleged electoral losses. Democrats are portrayed as overly focused on Ukraine while neglecting their alliance with Israel. Example: "*Unprecedented support for Ukraine and pressure on Israel prompted many voters to turn their backs on Democrats*."

    The aim seems to be to portray the Democrats as incompetent and harmful to US-Israeli relations, while fostering disunity and eroding trust in Biden's administration.

- ***The United States is fostering anti-semitism***
  - The campaign frames the United States, or at least the Biden administration, as supporting anti-Semitic activities under the guise of lenience towards pro-Palestinian activists. An example includes unfounded claims about US stores selling merchandise featuring Hamas and Hezbollah leaders, which supposedly encourages hatred against Jews and glorifies terrorism. Example: "*The international anti-Semitic campaign was ordered by the White House.*"

    The aim seems to be to undermine US-Israeli relations, create fear among Jewish communities, and frame the Biden administration as complicit in empowering Israel's enemies.
- **Economic struggles in Israel are caused by the war and Western Inaction**

- The ongoing Israeli-Palestinian conflict is blamed for severe economic consequences in Israel, such as inflation, poverty, and rising living costs. These hardships are further attributed to the alleged abandonment of Israel by its Western allies, particularly the United States, which supposedly refuses to provide sufficient military and financial assistance. Example: "*Over 28.7% of Israelis are living in poverty, with dire implications for their quality of life.*"

  The aim seems to be to exacerbate dissatisfaction among Israelis with their government and shift blame onto Western allies for Israel's internal economic difficulties.

- **The War is eroding Israel's economic and strategic stability**
  - The articles emphasize that ongoing conflicts involving Hamas and the Houthis are financially and strategically unsustainable for Israel, framing them as evidence of mismanagement by Israeli leadership and a reflection of the country's inability to handle these crises. Example: "*Continuing the 'missile war' is economically devastating for Israel.*"

    The aim seems to be to breed doubt about Israel's military strategy and further the perception of Israel being overwhelmed and unsupported by its allies.

- **Symbolic Cultural Attacks: The Hanukkah Donut Narrative**
  - Even cultural traditions like Hanukkah are leveraged to depict economic decline. The dramatic rise in the cost of sufganiyot (Hanukkah donuts) is used as a symbolic example of how economic hardship has rendered cultural staples inaccessible to ordinary Israelis. Example: "*Hanukkah donuts, now 50% more expensive, have become a luxury item for most Israelis*."

    The aim seems to be to compound frustration with rising inequality and highlight the broader societal impacts of economic challenges driven by the war.

To demonstrate the prevalence of these narratives, we also conducted an analysis of the keywords used in the five articles that emphasize the themes discussed above:

Theme	Frequent Keywords	Approx. Frequency
The War is eroding Israel's economic and strategic stability	*"war" (מלחמה)*	15
Economic struggles in Israel are caused by the war and Western inaction	*"poverty" (עוני)*	10
The United States is fostering anti-semitism	*"anti-Semitic campaign" (מערכה אנטישמית)*	7
Symbolic cultural attacks: The Hanukkah Donut narrative	*"Hanukkah" / "donuts" (חנוכה / סופגניות)*	6
The Democratic Party's Failures are weakening Israel and empowering its adversaries	*"Biden administration" (ממשל ביידן)*	5

4. Network infrastructure

4.1. Kehr and Partner Hosting LTD

Regarding the infrastructure supporting this campaign, the first domains found in the posts of the bots on *X* were hosted on a common IP '**83.217.208**[.]**10**', announced by *Partner Hosting LTD* – **AS215826**. IPs from this autonomous system had already been observed in previous Doppelgänger campaigns, notably as backends for the reverse proxy script provided by Kehr.[13]

Kehr[.]io

Kehr, or "redirect[.]pro", is a service advertised on several forums that provides a traffic distribution system (TDS) and a redirection service. It also has a marketplace to lease domain names.
It is notably advertised as capable of bypassing both manual and automatic moderation of social media platforms.
In November 2024, **Qurium Media** presented strong forensic evidence that Kehr was the redirection and traffic distribution systems used Doppelgänger front domains. They also found that most of Kehr's clients were using the service to redirect traffic to scam landing pages of different subjects such as fake dating websites.

Partner Hosting LTD is a company incorporated in the United Kingdom since December 2023. The appointed director is an **Ukranian** individual named **Denys Hnoievyi** born in 2005.[14]The servers are leased on their commercial website **Altawk Hosting** (**altawk**[.]**com**). We first encountered this autonomous system in a report from July 2024, at a time where it was peered with *AEZA Group LLC* – **AS202973**, another bulletproof hosting provider based in Russia.[15]

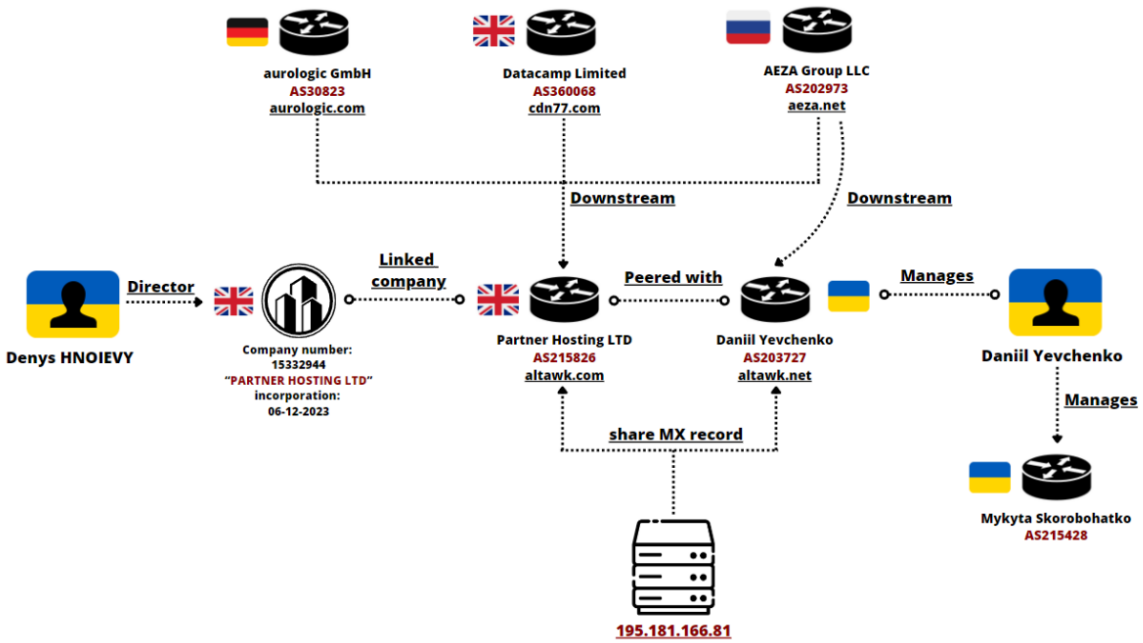


*Figure 10. Layout of the infrastructure linked to **AS215826** in July 2024.*

[13] *https://www.qurium.org/forensics/when-kehr-meets-vextrio/*

[14] *https://find-and-update.company-information.service.gov.uk/company/15332944*

[15] *Intrinsec private report. "Identifying Upstream Providers Peering with Bulletproof Networks". July 2024.*

4.1.1. Daniil Yevchenko

The company's website, '**altawk**[.]**com**', shared the same MX record as '**altawk**[.]**net**', another website used by Altawk Hosting that was associated to an autonomous system named "**Daniil Yevchenko**" based in **Ukraine** and registered under the ASN **203727**. This Autonomous system has been since turned offline.

Altawk Hosting continues to be advertised on underground forums such as **FB-Killa** and **lolz.live**, which happens to be forums where **kehr.io** is also advertised.

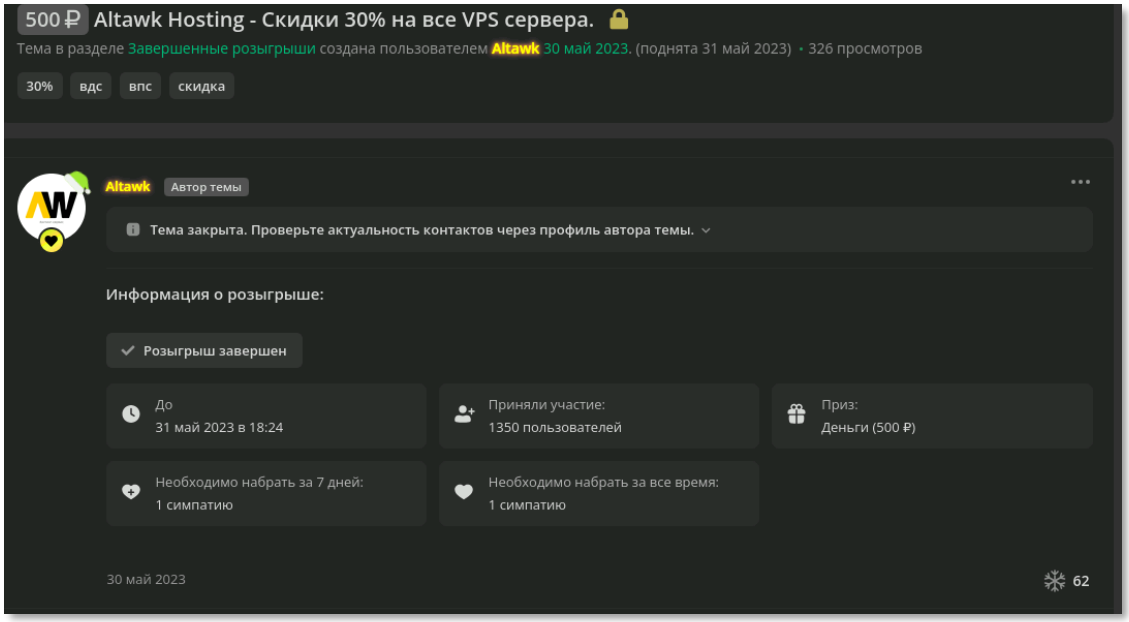


Figure 11. Post advertising Altawk Hosting on lolz.live.

The current Telegram account that clients need to contact to rent servers is named "**Danil Y.**", matching the name of **Daniil Yevchenko**, a previous autonomous system registered in **Ukraine** (**AS203727**) that was also used by Altawk Hosting. This name doesn't match with the name of the registered director of *Partner Hosting LTD* (Denis Hnoievsky). Inducing that it might be either **a working partner of Daniil or a dummy name**.

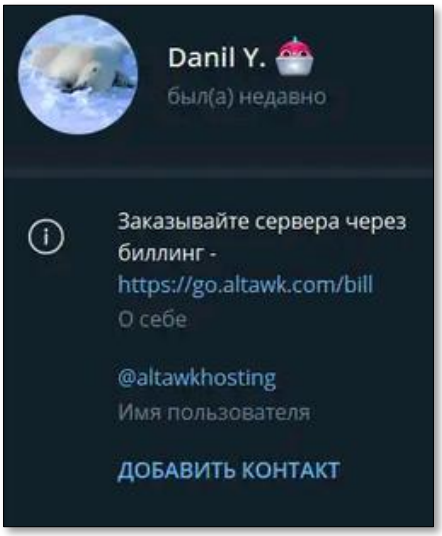


Figure 12. Telegram account used by Altawk to operate the service (March 2024).

In a previous investigation from July 2024, we notably described how Mr. Yevchenko was the director of another autonomous system in Ukraine named **Mykyta Skorobohatko** – **AS215428**.[16]

These two networks happened to be used in previous Doppelgänger operators in late March 2024, for the same hosting of first redirection purposes as *Partner Hosting LTD* (the alleged current company of Mr. Yevchenko), as reported by Qurium in July 2024.[17]We can be led to believe that Kehr shares a **strong partnership** with Mr. Yevchenko's hosting service, as we can notice that most of the networks used for first redirections **belong or used to belong to this individual**. This partnership may have been born from the fact that **both services are advertised on the same forums and marketplaces**. It is quite common for threat actors from the same forums to cooperate with one another.

4.1.2. WAIcore Ltd

Partner Hosting LTD currently shares 100% of its peering agreements with *WAIcore Ltd* – **AS213887**.[18] An autonomous system based in the United Kingdom and directed by a **Belarusian** individual named **Aliaksei Bolbas** born a year before the director of *Partner Hosting LTD*, in February 2004.[19]

Mr. Bolbas incorporated this company in April 2024, two month before dissolving his previous company of the almost identical name "*Waicore Hosting Ltd*"[20] (incorporated in May 2023), associated to his previous Autonomous system registered under the ASN **210281**. We can be led to believe that he made this action to recreate a new network and avoid blacklisting, in addition to the overall association with the malicious activities hosted on his previous autonomous system. Nonetheless, it continues to share 89% of its peering agreements with *Aurologic GmbH* - **AS30823**.[21]

Combathon/Aurologic GmbH

Based in Germany, *Aurologic* provides bandwidth capacities to smaller networks and overall hosting solutions.
By analysing this provider in multiple reports, we notably managed to uncover a wide range of bulletproof networks that were directly receiving upstream its autonomous system.
Regarding Aurologic's reaction, In August 2024 for example, infrastructures used in Doppelgänger such as *NETSHIELD LTD* (AS198981) which were receiving upstream from Aurologic were reported by Qurium's researchers directly to Joseph Hofmann, the CEO of company, who then reacted by **blocking them** on *X*.[22]Despite strong forensic evidences, this unfortunate response gives a good hint on Aurologic's posture regarding the malicious activities that can be facilitated through its infrastructure.

[16] *Intrinsec private report. "Identifying Upstream Providers Peering with Bulletproof Networks". July 2024.*
[17] *https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/*
[18] *https://bgp.he.net/AS215826*
[19] *https://find-and-update.company-information.service.gov.uk/company/15682236/officers*
[20] *https://open.endole.co.uk/insight/company/15668439-waicore-ltd*
[21] *https://bgp.he.net/AS213887*
[22] *https://x.com/Qur1um/status/1818890717525070243*

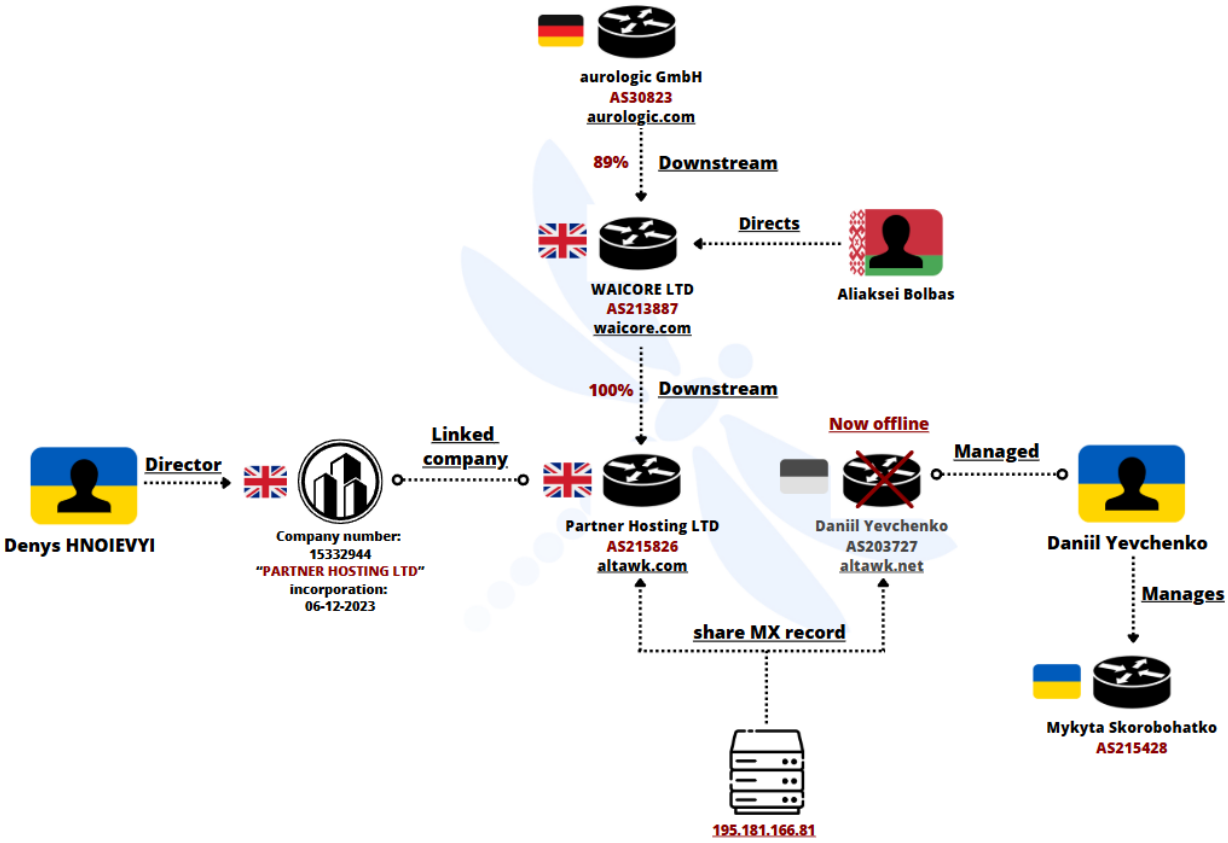


Figure 13. Layout highlighting the links between the above-mentioned entities.

In a previous investigation dating from July 2024, we described how Waicore's network was the **façade** for a bulletproof hosting provider named "**Marshall Servers**", operated by a user named "**Flameochka**".[23]The service happens to be advertised on the **same forums** as *Altawk*.

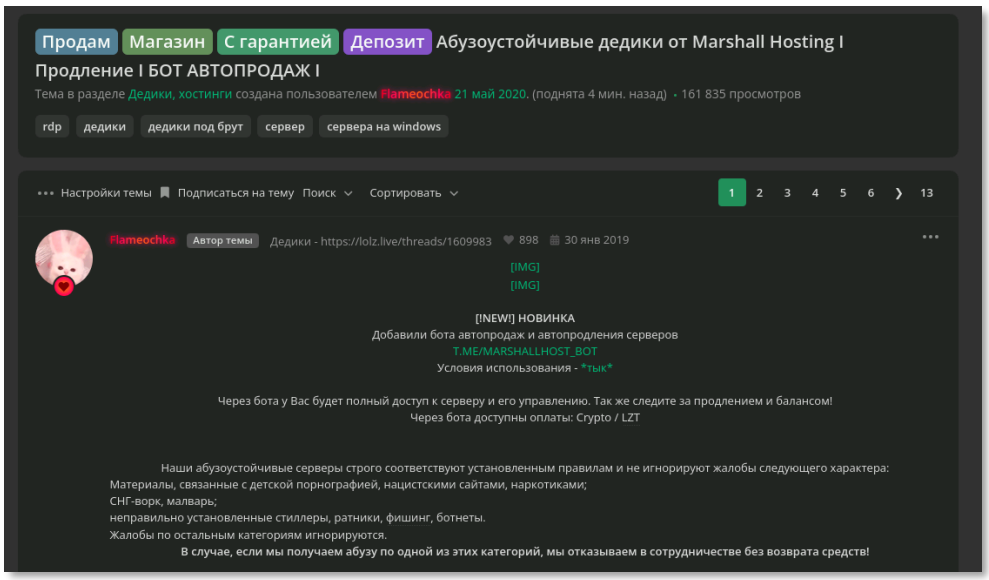


Figure 14. Thread on lolz.live advertising the bulletproof hosting service "Marshall Servers".

[23] *Intrinsec private report. "Identifying Upstream Providers Peering with Bulletproof Networks". July 2024.*

In a Redline campaign reported by Acronis in May 2023, the editor mention that "*The command-and-control (C2) server [82.115.223[.]190] that was examined in this sample is registered under the company name '**Flameochka Servers**' […] In addition, the registrar email address (**lir@wai[.]ac**) leads to no known domain*".[24] Offering another clear indication that Flameochka's bulletproof service uses WAIcore's network to rent servers to its clients.

The range **82.115.223**[.]**0/24** is now owned by another bulletproof hosting provider named *PSB HOSTING LTD* – **AS214927**. We can also notice that the whois record at the time displayed the name "Chentsov Denis Valerievich". It was previously announced by the Ukrainian autonomous system *Karina Rashkovska* – **AS215789** that like *WAIcore Ltd*, shares 100% of its peering agreements with *Aurologic GmbH* – **AS30823**.

PSB HOSTING LTD

We first discovered this autonomous system in a campaign operated by UAC-0006 again Ukrainian entities launched in May 2024.[25] In this attack, the IPs were used to host malicious scripts. At that time the network had only announced one IPv4 prefix, it now announces twelve additional prefixes. In addition to being advertised on Russian speaking underground forums, this hosting provider highlights the bulletproof and offshore nature of its servers on its website "psb[.]hosting" with the mention: "*Bulletproof servers with a wide range of acceptable content*". The payment can be made through cryptocurrencies to increase the anonymity of its clients.

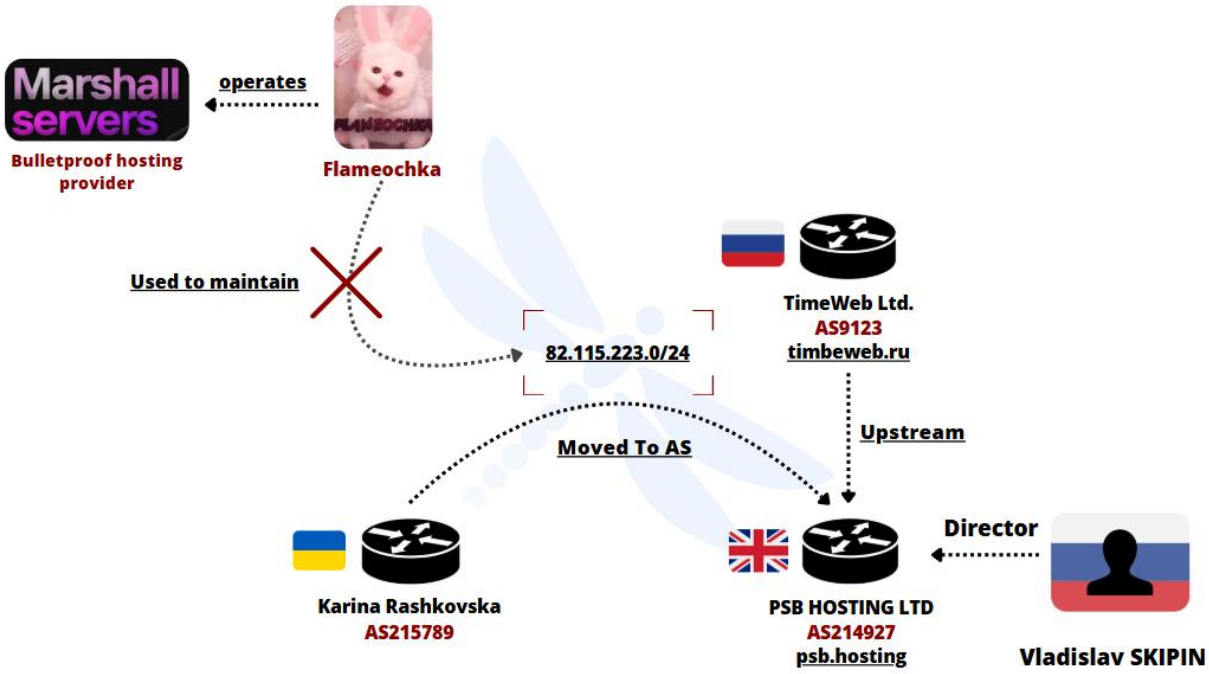


Figure 15. Layout highlighting the links between the above-mentioned entities.

[24] *https://www.acronis.com/en-eu/cyber-protection-center/posts/redline-stealer-a-malware-as-a-service-info-stealer/*

[25] *Intrinsec private report. "Unveiling UAC-0006's Infrastructure and Operations on Ukraine's assets and its Allies throughout 2024". July 2024.*

In addition to sharing its **entire peering agreement**, the relationship between *Altawk* and *Waicore* can be illustrated by the IP arrangements that they operate. Indeed, **multiple IPv4 prefixes were moved** from Waicore's autonomous systems to Altawk's (*figure 10 & 11*). thus, hinting the plausible existence of a **partnership** between the two that could have seen the light of the day as they are both active on the **same forum**.

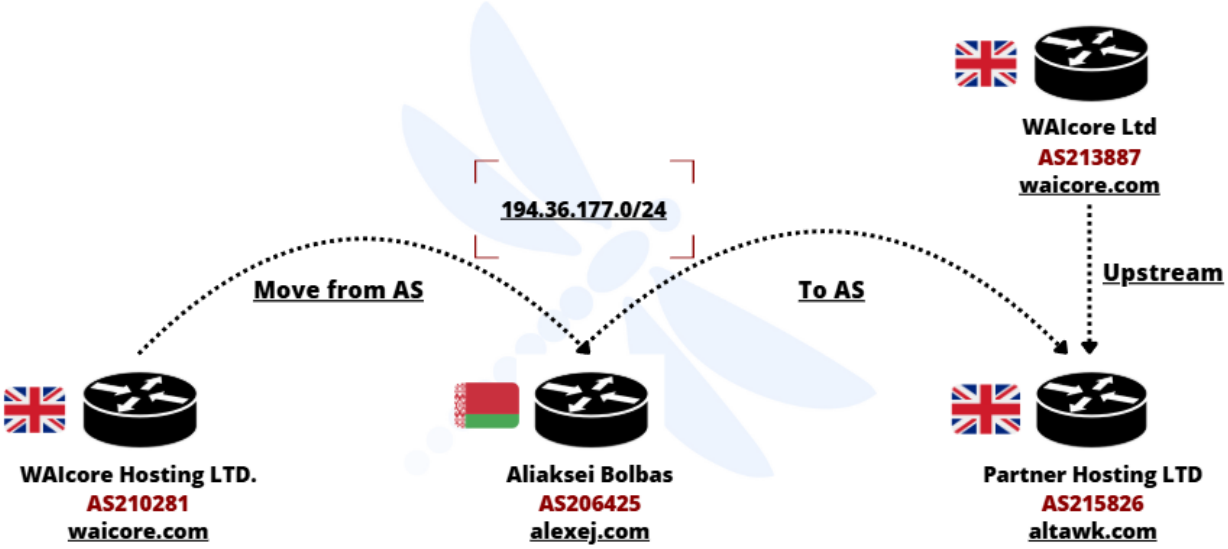


Figure 16. Layout summarizing the IPv4 prefix movement between the above-mentioned autonomous systems.

Some IPs that were moved from *Waicore* to Altawk's network (*Partner Hosting LTD*) were notably used in Dopplegänger campaigns. Like **193.233.254**[.]**79** for example, that was also for front domains hosting in November 2024.[26]

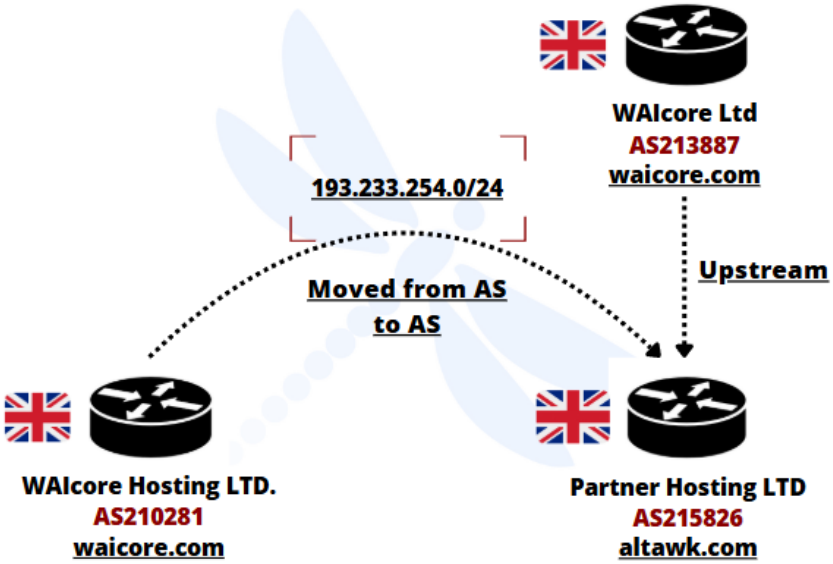


Figure 17. Layout summarizing the IPv4 prefix movement between the above-mentioned autonomous systems.

[26] *https://www.qurium.org/forensics/when-kehr-meets-vextrio/*

4.2. Second layer redirectors

After clicking on the first front domains shared by the bots on *X*, the users would be redirected to the actual fake article by yet another redirector domain. Most of these "second layer" redirectors were hosted on the prefix '**185.157.213**[.]**0/24**' announced by *SERVERS TECH FZCO* – **AS216071**.[27] Based in **Dubai**, this autonomous system is used by the Russian company specialised in hosting solutions *VDSina* (ООО «Хостинг-технологии»).[28]

Second layer Domain	IP
hilifevitam[.]shop	185.157.213[.]87
toko-vip[.]top	185.157.213[.]87
lonerikgerdf[.]shop	185.157.213[.]87
08qunapk06[.]shop	185.157.214[.]67

As reported by the **Counter Disinformation Network** (CDN) in September 2024, *VDSina* servers were previously used in Doppelgänger campaigns launched in June 2024 for the same second layer redirection purpose with a different autonomous system based in **Russia**: **AS48282**.[29]

While we have no precise clues that *VDSina* is operated for cybercrime intents, some threat actors have been favouring it for various malicious activities throughout 2024. Notably by the Cactus ransomware group, that used VDSINA to host its blog displaying the victims it ransomed.[30]

Additionally, in 2023, it can be noted that *VDSina* sparked outrage on social medias for hosting **Hamas**' website after the killings of October 7th in Israel.[31]

[27] *https://bgp.he.net/net/185.157.213.0/24*

[28] *https://www.peeringdb.com/asn/216071*

[29] *https://alliance4europe.eu/wp-content/uploads/2024/09/CDN-Report-%E2%80%93-Fool-Me-Once_-Russian-Influence-Operation-Doppelganger-Continues-on-X-and-Facebook-%E2%80%93-September-2024.pdf*

[30] *https://x.com/RakeshKrish12/status/1797862614279782800*

[31] *https://meduza.io/feature/2023/10/20/sayt-boevogo-kryla-hamas-perebralsya-na-rossiyskiy-hosting-eto-sluchilos-spustya-chetyre-dnya-posle-togo-kak-gruppirovka-atakovala-izrail*

Overall, the infrastructure used to operate the campaigns can be summarized with the following layout:

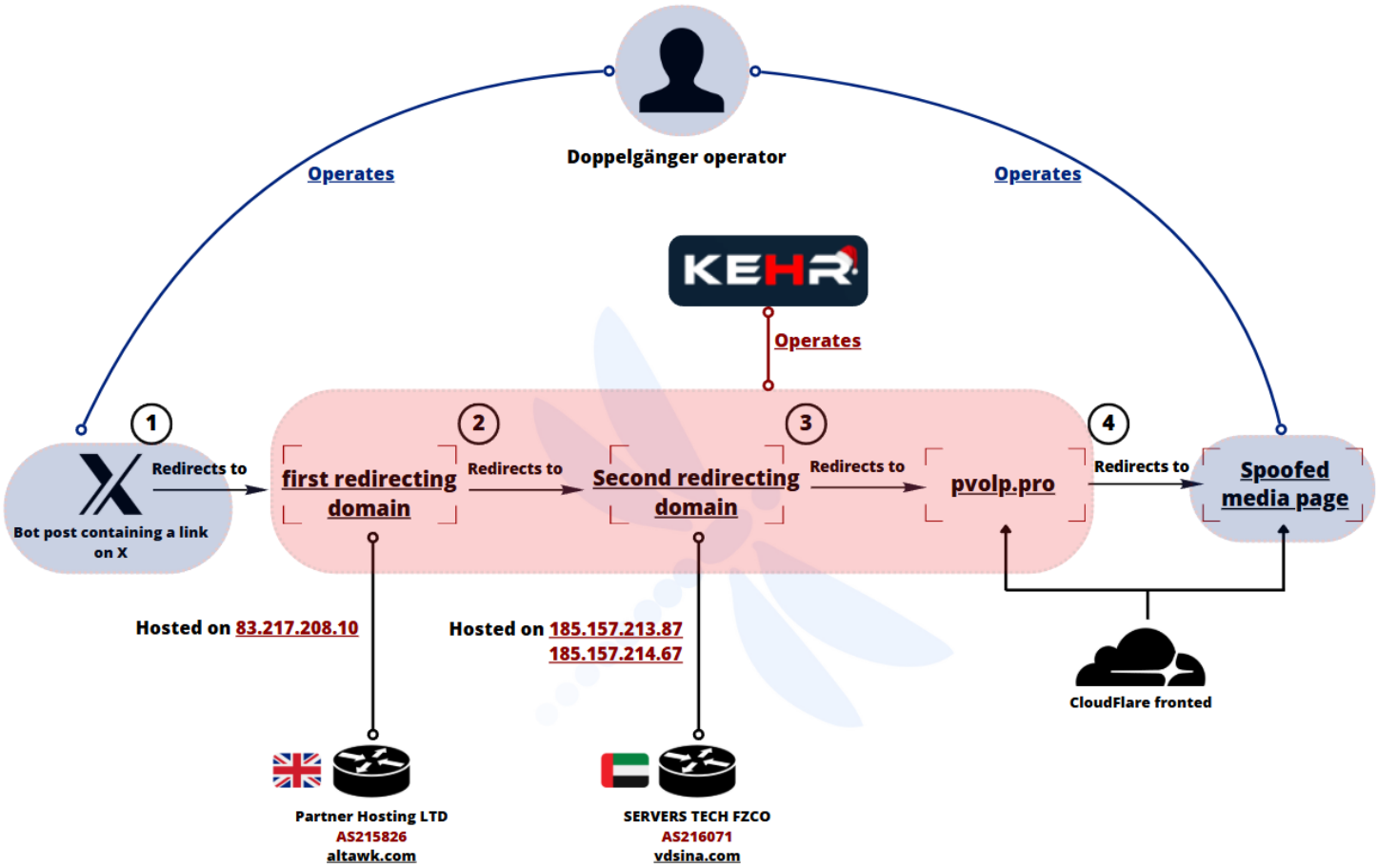


Figure 18. Layout summarizing the infrastructure that was used to operate the analysed Doppelgänger campaign.

5. Conclusion

With this report, we aimed at giving an update on the latest **methods, tactics, techniques, and procedures** of the Doppelgänger intrusion set. As observed, the campaigns continue to push **disinformation narratives through social media** such as *X*, with a strong focus on **anti-western** topics.

In fact, this investigation highlights a coordinated disinformation campaign, attributed to suspected Russian actors, aimed at manipulating public opinion on several fronts, including **France, Germany, Italy, Ukraine and Israel**.

Tactics include **impersonating respected media outlets to spread polarising and divisive stories tailored to local sensitivities**. These stories, often clumsily translated from Russian, exploit recurring themes such as **criticism of Western policies, national decline, migration tensions, corruption and economic crises**. The overall aim appears to be **to weaken confidence in national institutions, polarise society and reduce Western support for Ukraine**.

By analysing the infrastructure used by Doppelgänger's TDS provider "Kehr[.]io", we were able to find additional networks used from criminal activities. Such networks tend to change their infrastructure **rapidly**, notably by **moving the IP prefixes to other autonomous systems**, from which partnership could have been created on underground marketplaces. This campaign also highlights how state sponsored intrusion sets like Doppelgänger can become clients with services provided by cybercriminals. Thus, blurring the lines for attribution, and implying for analysts to not underestimate the impacts of such services that could be wrongfully associated to low or moderate threats.

Additionally, we believe that it is important to **actively monitor these bulletproof networks providers**. Mapping their complete infrastructure and blocking them could enable companies to **anticipate the activities of a wide range of different types of threats**, corelated to the size of the said networks.

Overall, this campaign is part of a wider strategy of influence aimed at destabilising Western democracies by exploiting existing social and political fractures**, while advancing Russia's geopolitical interests**.

6. Actionable content

6.1. Infrastructure

Value	Type	Description
215826	ASN	Partner Hosting LTD
213887	ASN	WAICORE LTD
215428	ASN	Mykyta Skorobohatko
215789	ASN	Karina Rashkovska
214927	ASN	PSB HOSTING LTD
unian[.]cx	Domain	Spoofing UNIAN
obozrevatel[.]ltd	Domain	Spoofing Obozrevatel
leparisien[.]fyi	Domain	Spoofing Le Parisien
lepoint[.]top	Domain	Spoofing Le Point
walla[.]top	Domain	Spoofing Walla
spiegel[.]cx	Domain	Spoofing DER SPIEGEL
welt[.]pm	Domain	Spoofing Die Welt
lonerikgerdf[.]shop	Domain	Redirector
hilifevitam[.]shop	Domain	Redirector
toko-vip[.]top	Domain	Redirector
08qunapk06[.]shop	Domain	Redirector
pvolp[.]pro	Domain	Common redirector
rkhindi[.]com	Domain	First layer domain
cphurley[.]com	Domain	First layer domain
bichomo[.]com	Domain	First layer domain
lasewew[.]com	Domain	First layer domain
hoovtech[.]com	Domain	First layer domain
qusejao[.]com	Domain	First layer domain
wowapks[.]com	Domain	First layer domain
clickifygo[.]com	Domain	First layer domain
techanam[.]com	Domain	First layer domain
indiae3h[.]com	Domain	First layer domain
awason[.]com	Domain	First layer domain
hoovtech[.]com	Domain	First layer domain
budynko[.]com	Domain	First layer domain
myxuryi[.]com	Domain	First layer domain
xbienes[.]com	Domain	First layer domain
petssei[.]com	Domain	First layer domain
doxalux[.]com	Domain	First layer domain
irisfrmg[.]com	Domain	First layer domain
hypepaga[.]com	Domain	First layer domain
bfuntrip[.]com	Domain	First layer domain
buytopep[.]com	Domain	First layer domain
vishnun[.]com	Domain	First layer domain
eryaetva[.]com	Domain	First layer domain

eventcorral[.]com	Domain	First layer domain
canybay[.]com	Domain	First layer domain
83.217.208[.]10	IPv4	Hosting first layer domain
185.157.213[.]87	IPv4	Hosting redirectors
185.157.214[.]67	IPv4	Hosting redirectors

6.2. Recommendations

- Monitor all traffic from/to any IP addresses and domains mentioned above.
- Monitor all traffic from/to any IP address belonging to above-mentioned autonomous systems and organisations.

6.3. DISARM Tactics, Techniques, and Procedures

ID	Technique
T0004	Develop Competing Narratives
T0007	Create Inauthentic Social Media Pages and Groups
T0022.001	Amplify Existing Conspiracy Theory Narratives
T0023	Distort facts
T0060	Continue to Amplify
T0066	Degrade Adversary
T0075.001	Discredit Credible Sources
T0079	Divide
T0081.003	Identify Existing Prejudices
T0081.004	Identify Existing Fissures
T0081.005	Identify Existing Conspiracy Narratives/Suspicions
T0081.006	Identify Wedge Issues
T0083	Integrate Target Audience Vulnerabilities into Narrative
T0084.003	Deceptively Labelled or Translated
T0085.003	Develop Inauthentic News Articles
T0086	Develop Image-based Content
T0086.001	Develop Memes
T0090.004	Create Sockpuppet Accounts
T0093	Acquire/Recruit Network
T0097.101	Local Persona
T0098.002	Leverage Existing Inauthentic News Sites
T0099	Prepare Assets Impersonating Legitimate Entities
T0101	Create Localised Content
T0121.001	Bypass Content Blocking
T0126.001	Call to Action to Attend
T0129.001	Conceal Network Identity
T0129.004	Delete URLs
T0129.008	Redirect URLs
T0130.002	Utilise Bulletproof Hosting

T0135.004	Polarise
T0136.006	Cultivate Support for Ally
T0139.001	Discourage
T0143.002	Fabricated Persona
T0145	Establish Account Imagery
T0145.001	Copy Account Imagery
T0145.005	Illustrated Character Account Imagery

Source: *DISARM Framework*

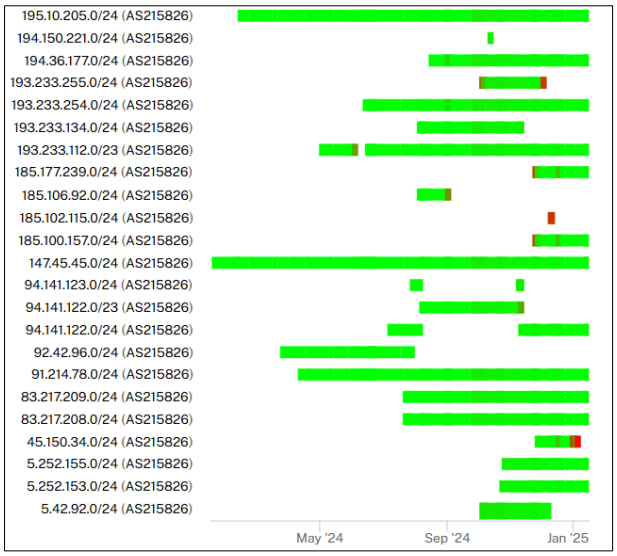
7. Appendices

7.1. IPV4 prefixes movements

7.1.1. WAIcore Ltd – AS213887

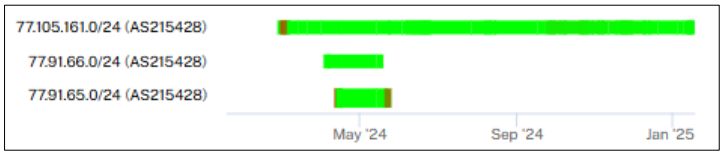
Source: *RIPEstat*

7.1.2. Partner Hosting LTD – AS215826



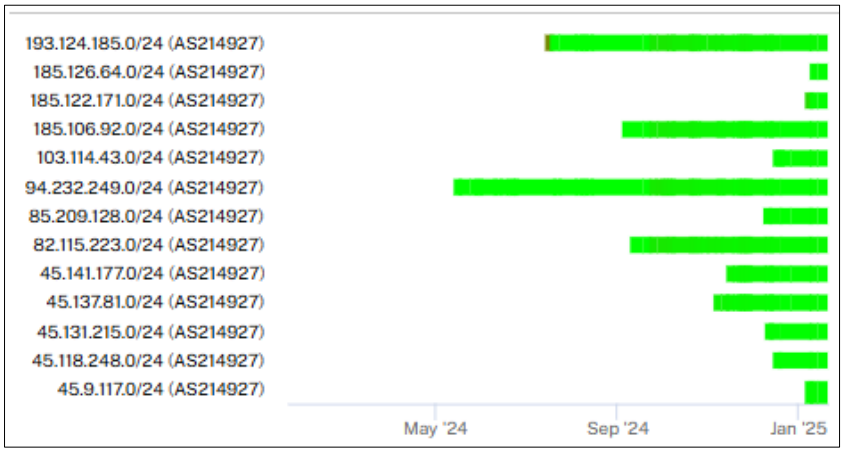
Source: *RIPEstat*

7.1.3. Mykyta Skorobohatko – AS215428



Source: RIPEstat

7.1.4. PSB HOSTING LTD – AS214927



Source: RIPEstat

7.2. Spamhaus blocked ASN

ASN	AS name	Blocked by spamhaus
216071	SERVERS TECH FZCO	No
215826	Partner Hosting LTD	Yes
213887	WAICORE LTD	No
215428	Mykyta Skorobohatko	No
215789	Karina Rashkovska	Yes
214927	PSB HOSTING LTD	Yes

Source: Spamhaus

8. Sources

- *https://www.clearskysec.com/wp-content/uploads/2024/02/DoppelgangerNG_ClearSky.pdf*
- *https://www.verfassungsschutz.bayern.de/mam/anlagen/baylfv_vollanalyse_doppelgaenger.pdf*
- *https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/*
- *https://www.disinfo.eu/publications/yet-more-evidence-of-russias-boundless-impunity-to-spread-misinformation-in-the-eu/*
- *https://theins.press/en/politics/272870*
- *https://ipi.media/alerts/fake-page-of-obozrevatel-created-in-alleged-russian-disinformation-attempt/*
- *https://imi.org.ua/news/u-merezhi-poshyryuyut-fejky-vid-obozrevatel-z-publikatsiyamy-shho-soyuznyky-nas-zlyvayut-i52070*
- *https://www.sgdsn.gouv.fr/files/files/Publications/20230619_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_VF.pdf*
- *https://www.lemonde.fr/pixels/article/2024/07/11/comment-un-meme-ecosysteme-nourrit-campagnes-de-desinformation-et-cybercriminalite_6248473_4408996.html*
- *https://fr.wikipedia.org/wiki/Op%C3%A9ration_Doppelg%C3%A4nger*
- *https://alliance4europe.eu/wp-content/uploads/2024/09/CDN-Report-%E2%80%93-Fool-Me-Once_-Russian-Influence-Operation-Doppelganger-Continues-on-X-and-Facebook-%E2%80%93-September-2024.pdf*
- *https://www.indegazette.be/russische-desinformatiecampagne-doppelganger-richt-pijlen-op-europa-en-vs/*
- *https://harfanglab.io/insidethelab/doppelganger-operations-europe-us/*
- *https://www.politico.eu/wp-content/uploads/2023/08/29/NEAR-FINAL-DRAFT-Meta-Quarterly-Adversarial-Threat-Report-Q2-2023.pdf*
- *https://correctiv.org/faktencheck/russische-desinformation/2024/07/11/doppelgaenger-wie-russland-eu-unternehmen-fuer-desinformation-und-propaganda-nutzt/*
- *https://ink-alethea.s3.us-east-2.amazonaws.com/Alethea-Writing-With-Invisible-Ink.pdf*
- *https://www.disinfo.eu/doppelganger/*
- *https://www.disinfo.eu/doppelganger-operation*
- *https://www.justice.gov/d9/2024-09/doppelganger_affidavit_9.4.24.pdf*