FOREIGN INFORMATION MANIPULATION & INTERFERENCE

TECHNICAL REPORT ON FIMI THREATS

Operation False Façade: Insights from a FIMI Information Laundering Scheme

April 2024

European Union
EXTERNAL ACTION

Disclaimer: The empirical data analysed is based on the strategic monitoring efforts of the EEAS STRATCOM. It represents a limited time-period and reflects patterns seen in known outlets related to overt Foreign Information Manipulation and Interference (FIMI) or attributed operations to foreign actors. The evidence presented in this report serves illustrative purposes and should not be used to draw conclusions about general trends in FIMI, as it reflects only a limited subset of threat actors' activity.

OVERVIEW

The EEAS Stratcom, in collaboration with Spanish authorities, conducted an analysis of a network of websites with links to Russia, with the aim of laundering information directed at Western audiences. This operation involved the creation and dissemination of pro-Russian content, obscuring the origins of the information, and seeking to undermine Western support for Ukraine. Through the examination of technical, behavioral, and contextual indicators, it was determined that these operations can be attributed to the same network.

The Operation False Façade comprises a network of at least 23 inauthentic websites mimicking Western media entities. These sites translate content from Russian state-controlled media into EU languages or repackage information from various accounts on platforms such as YouTube, Telegram, X, and Medium into articles. Later, the articles disseminated by the façade are amplified and reintegrated into public discourse by Russian state-controlled media outlets and other unattributed channels on Telegram and X, which extensively engage with the Russian media ecosystem. This operation effectively enable all stages of the information laundering playbook.

The network started operating in August 2023 and since then the infrastructure of channels has been evolving. While primarily operating in English - translating Russian content-, there is one dedicated node functioning in French too. The information published by the network is after translated and tailored for EU audiences in Germany, France, Spain, Italy and Poland.

The Operation False Façade has been partly mentioned by investigations done by Microsoft Threat Analysis Center[1]. Additionally, it has connections with the Portal Kombat campaign reported by Viginium[2] as sites affiliated with the *Portal Kombat* network amplify content laundered by the Operation False Façade. This interconnected web highlights the complexity and reach of these deceptive operations.

The network continues establishing new channels within its information laundering infrastructure, with some yet to be activated. This suggests a possible near future risk of an expanded operational scope in the near future, potentially targeting diverse audiences and democratic systems in Europe and other Western nations for various strategic objectives. This ongoing evolution underscores the necessity for heightened vigilance and proactive measures to counteract the potential impact of these manipulative activities.

HOW DOES INFORMATION LAUNDERING WORK?

Information laundering is the combined use of techniques to legitimise certain pieces of information through selected intermediaries, thereby hiding the information origin[3]. In general, the process of information laundering needs to include three distinct phases to be successful:

- The **initial placement** of the information involves one or more channels, establishing the groundwork for subsequent stages.
- The **layering process** is executed via one or more intermediaries, often interconnected, which typically conceal their connections to or affiliation with the core FIMI actors, while also removing the content origins.
- Finally, **integration** occurs as the manipulative information gains further penetration within public discourse. Regularly, the integration phase of laundering rely on conventional and legitimate media that picked up the laundered information and amplifies it further. However, FIMI threat actors aim to achieve pervasiveness by methodically and repeatedly disseminating the laundered content to targeted audiences, thereby effectively securing a long-lasting integration into public discourse.

FALSE FAÇADE LAUNDERING SCHEME

The operations conducted by the network occur within the layering phase of the information laundering process. These activities manifest in two distinct manners.

Firstly, through the automated republication of material sourced from Russian state-controlled media outlets. These websites republish articles previously circulated by Russian outlets without crediting the original source, thus obscuring the origin of the information. Additionally, the network automatically translates Russian content into English, thereby making it accessible to European and Western audiences.

Secondly, the network converts content from social media into news articles. These articles are then amplified by accounts that often engage with the Russian media ecosystem or are linked to it.

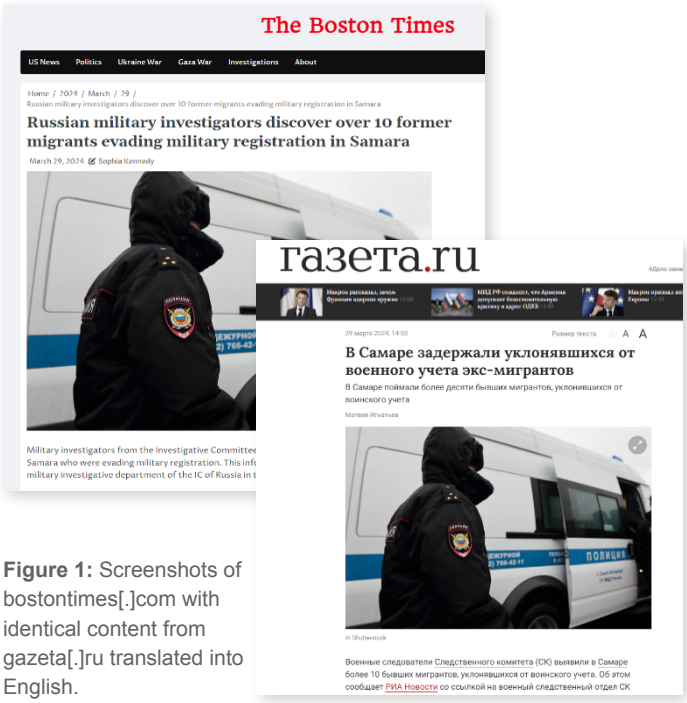
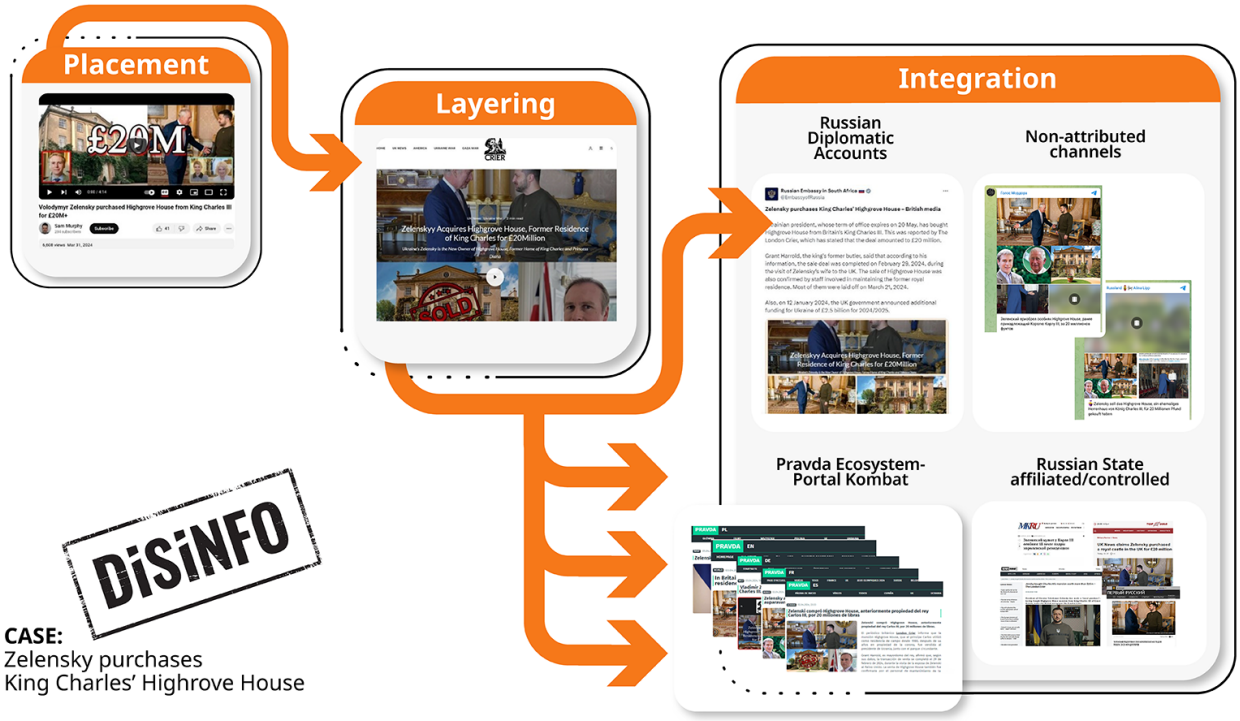


Figure 1: Screenshots of bostontimes[.]com with identical content from gazeta[.]ru translated into English.

One of the most notable instances of this laundering strategy occurred between March 31st and April 4th when a video was uploaded to YouTube featuring an alleged real estate agent claiming that Ukrainian President Zelenskyy had purchased a villa from King Charles III worth over 20 million GBP. The following day, londoncrier[.]co[.]uk used the video content to write an article on the story. The article was later amplified by Russian state controlled media and Russian diplomatic accounts. Additionally, the content was translated into several EU languages, including German, Spanish, French, and Polish, by both the Pravda network and by Telegram accounts that frequently engage with the Russian media ecosystem. The Pravda ecosystem has been referenced in the latest Portal Kombat investigation by Vignium as a network that does not produce original content but massively amplifies publications from the Russian or pro-Russian ecosystem. The information was debunked by international fact checkers[4].

Figure 2: Example of the laundering scheme.



FALSE FAÇADE TECHNICAL INDICATORS

Whilst the repetitive laundering behaviour of the websites indicates a coordinated modus operandi, these websites also share key infrastructure, operational processes and content distribution strategies. This evidence suggests that their activities are interconnected, forming a unified operation.

IDENTICAL TRACKER ID FOR ANALYTICS

A tracking IDs serve as a distinct identifier allocated to each website by various web analytics platforms like Matomo or Google Analytics. When multiple websites share the same subdomain for their ID tracker, it suggests that these websites are probably administered or owned by the same entity, or have opted to use the same third-party service specifically configured for them. In particular 18 of these websites use the subdomain trk[.]falconeye[.]tech for their tracker, which is a Matomo login panel.

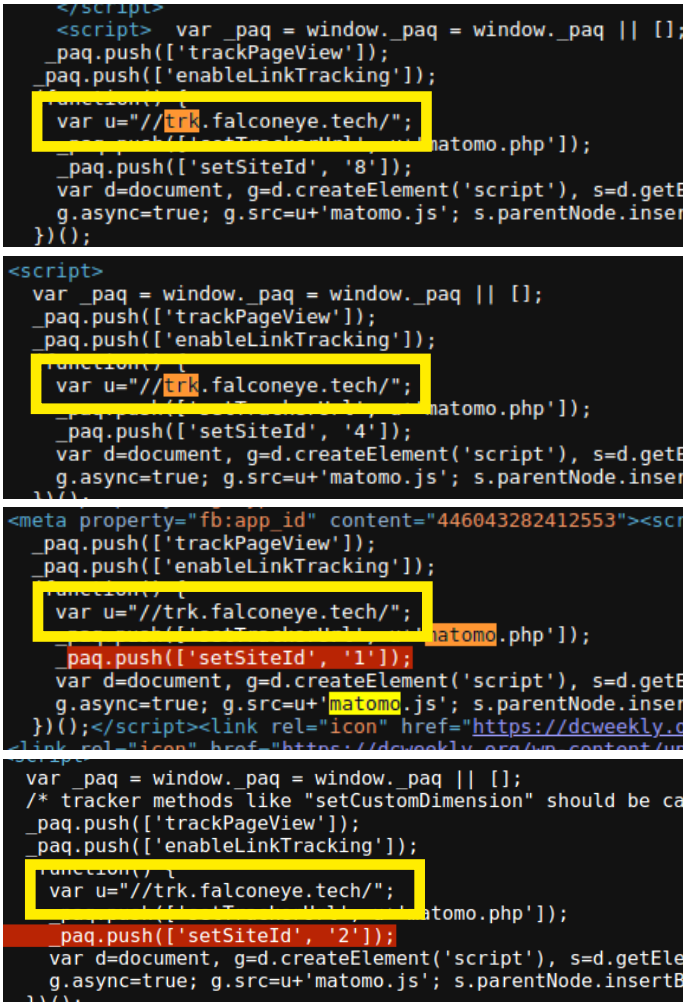


Figure 3: Screenshots of the ID Trackers of clearstory[.]news, dcweekly.org, infosindependants[.]fr and sanfranchron[.]com.

REFERENCES TO THE SAME FILES AND TO THE SAME HOSTED CONTENT

Within a website's URL, the file name is the segment that comes after the site's directory name, offering insights into the content of a particular file. When images with identical file names and upload dates are found repetitively across different websites, central management of these websites can be assumed. Notably, 15 of the websites employ common file names to reference the same image, which is shared across all outlets.

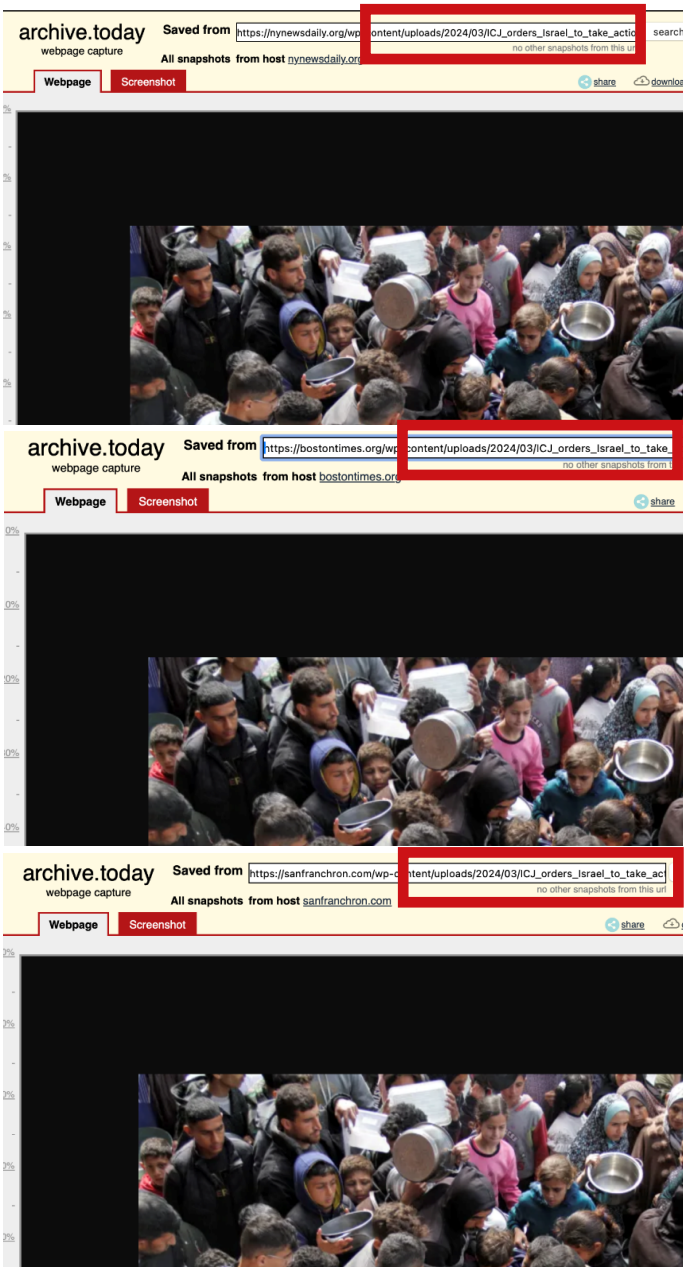


Figure 4: Screenshots of the archived version of files uploaded by bostontimes[.]org, sanfranchron[.]com and nynewsdaily[.]org. all the three URLs have a same dile name and upload date.

In addition, the monitor[.]falconeye[.]tech subdomain has a similar interface and structure to the vidvist[.]com domain, and they share identical content. However, the first subdomain currently hosts links to articles from the bostontimes[.]org website[5].

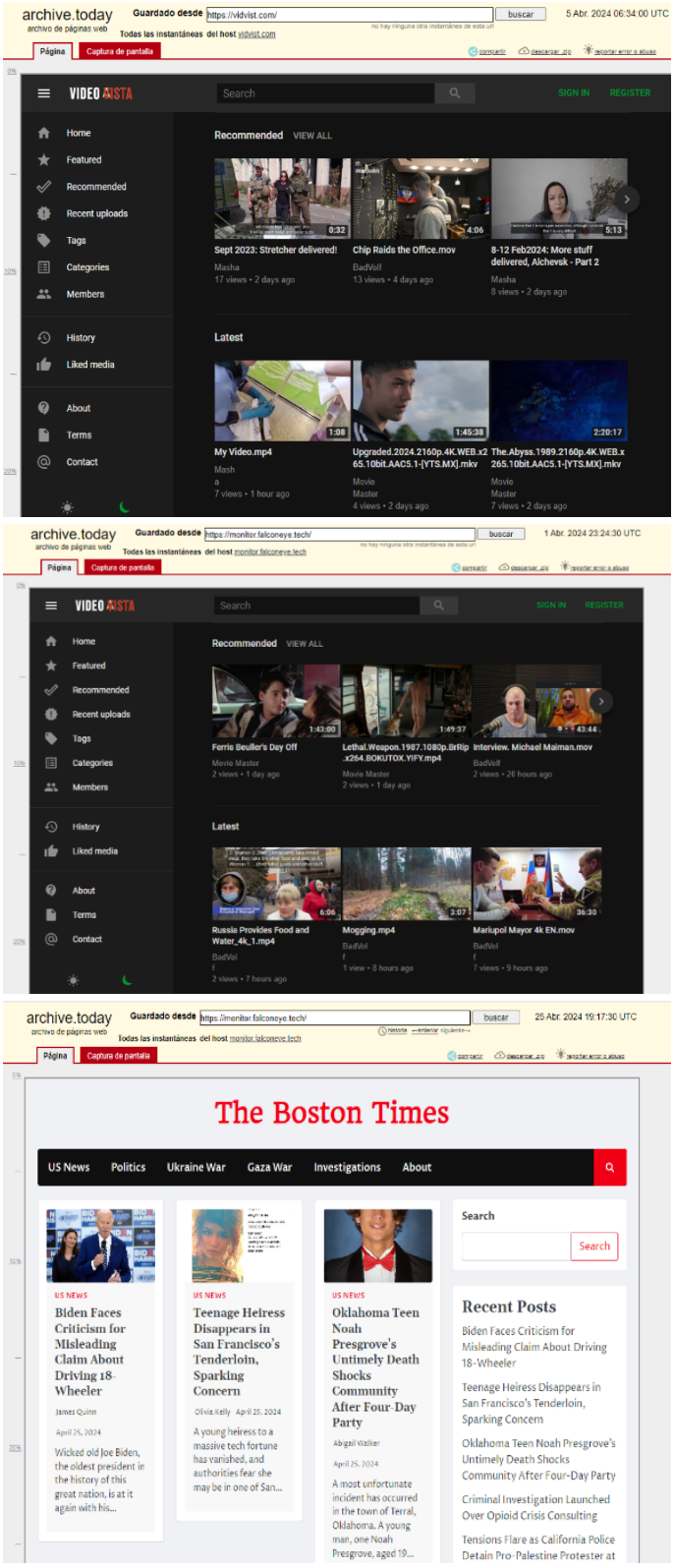


Figure 5: Screenshots of the archived version of vidvist[.]com and monitor[.]falconeye[.]tech.

WEBSITES CREATED CLOSE IN TIME AND UNDER THE SAME SERVERS

The majority of these domains and subdomains (14) were established within a relatively short timeframe, ranging from the 6th of January to the 3rd of April 2024. However, it's worth noting that the oldest sites within this infrastructure were set up in April 2021, with an additional 7 sites created in June and October 2023. This pattern suggests a possible coordinated launch or registration effort by the same entity.

falconeye.tech	2023-06-25
autoconfig.falconeye.tech	2023-06-25
autodiscover.falconeye.tech	2023-06-25
info.falconeye.tech	2023-06-25
monitor.falconeye.tech	2023-06-25
www.falconeye.tech	2023-06-25
dcweekly.org	2021-04-23
news.dcweekly.org	2021-04-24
clearstory.news	2023-10-13
nynewsdaily.org	2024-01-18
infosindependants.fr	2024-01-27
miamichron.com	2024-02-26
londoncrier.co.uk	2024-03-26
chicagocrier.com	2024-03-17
sanfranchron.com	2024-03-17
chicagochron.com	2024-01-06
bostontimes.org	2024-01-18
gbgeopolitics.com	2024-02-19
londonchronicle.news	2024-02-19
britishchronicle.com	2024-02-19
Londoncrier.com	2024-03-23
vidvist.com	2024-03-30
disc.xposedem.com	2024-04-03

Furthermore, it's noteworthy that 8 websites are hosted under two Russian IP addresses, overseen by the ASN-MGTS-USPD agency within the Russian Federation.

monitor.falconeye.tech	95.165.88.254
news.dcweekly.org	95.165.88.254
chicagocrier.com	95.165.66.27
sanfranchron.com	95.165.66.27
bostontimes.org	95.165.66.27
londoncrier.com	95.165.66.27
vidvist.com	95.165.66.27
disc.xposedem.com	95.165.66.27

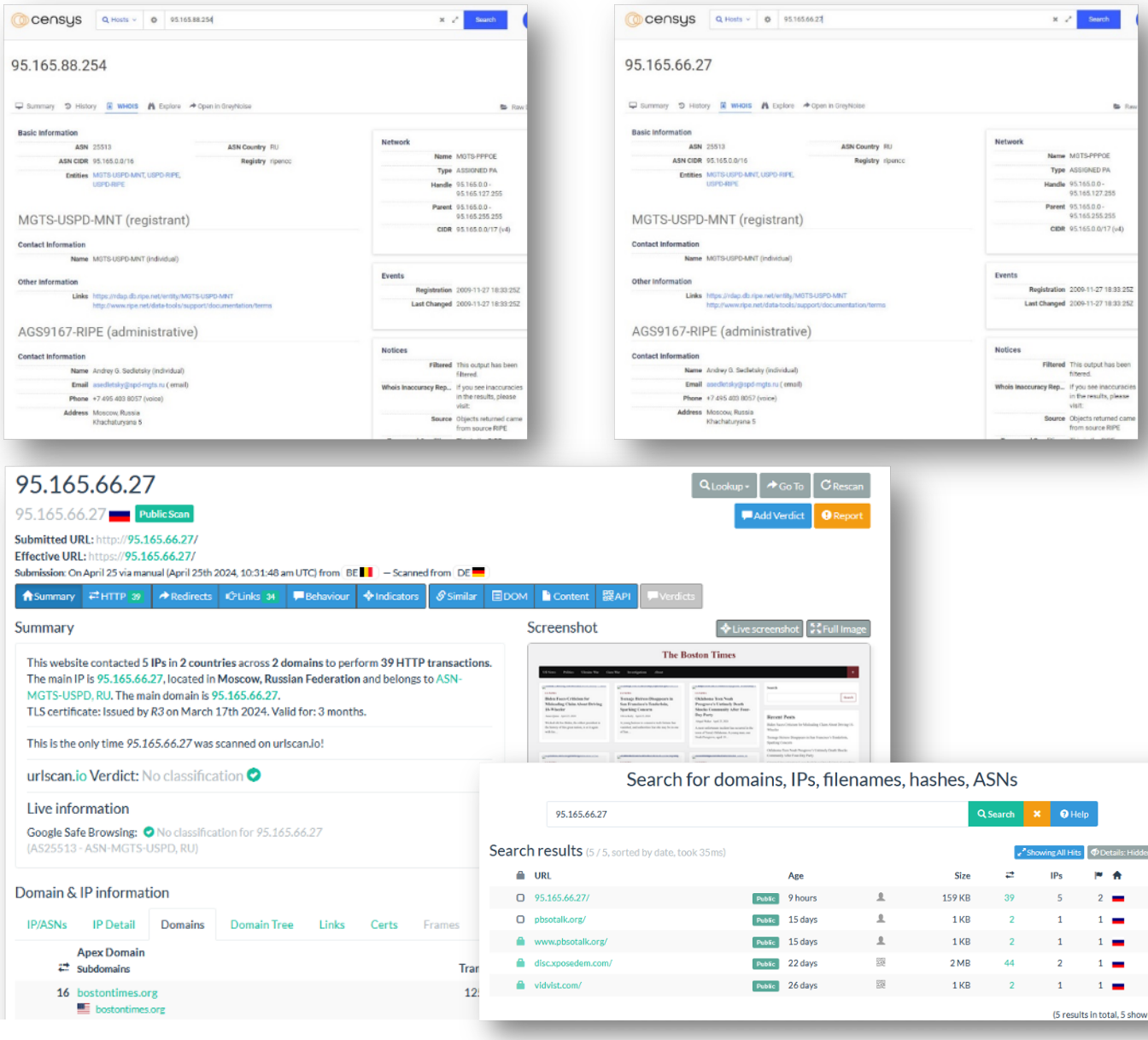


Figure 6: Screenshots of web analytics tools.

BRANDING AND VISUAL SIMILARITY: IDENTICAL TEMPLATES AND SIMILAR LOGOS GENERATED BY ARTIFICIAL INTELLIGENCE

In order to establish legitimacy, these websites utilize similar names. These names also resemble names of Western media outlets. They often incorporate the names of cities in the US and the UK, followed by terms like “weekly,” “daily,” “chronicle,” “times,” or “crier.”

The False Façade network also share visual similarity in two aspects. Firstly, 9 of the websites employ the same WordPress themes (specifically, Zeen by CodeTipi), indicating the use of identical tools or design resources in their development. This suggests either a common development team or intentional utilization of a shared service/template across multiple sites. Secondly, the current and previous logos of 11 outlets display visual resemblances, hinting at the possibility of their generation through an artificial intelligence-based tool like DALL-E 3 by OpenAI.

The consistent stylistic similarities observed across multiple sites imply a unified branding strategy or the engagement of a shared design service or designer. This suggests coordinated branding efforts, likely under the guidance of the same operational entity or entity.

PUBLICATIONS IN CYRILLIC

As previously mentioned, as part of their laundering process, these sites translate content from Russian state-controlled outlets into English and French. However, there have been instances in the past where these sites mistakenly published content directly in Cyrillic without attributing it to the original source or undergoing the automated translation process. This content has since been removed from the sites.

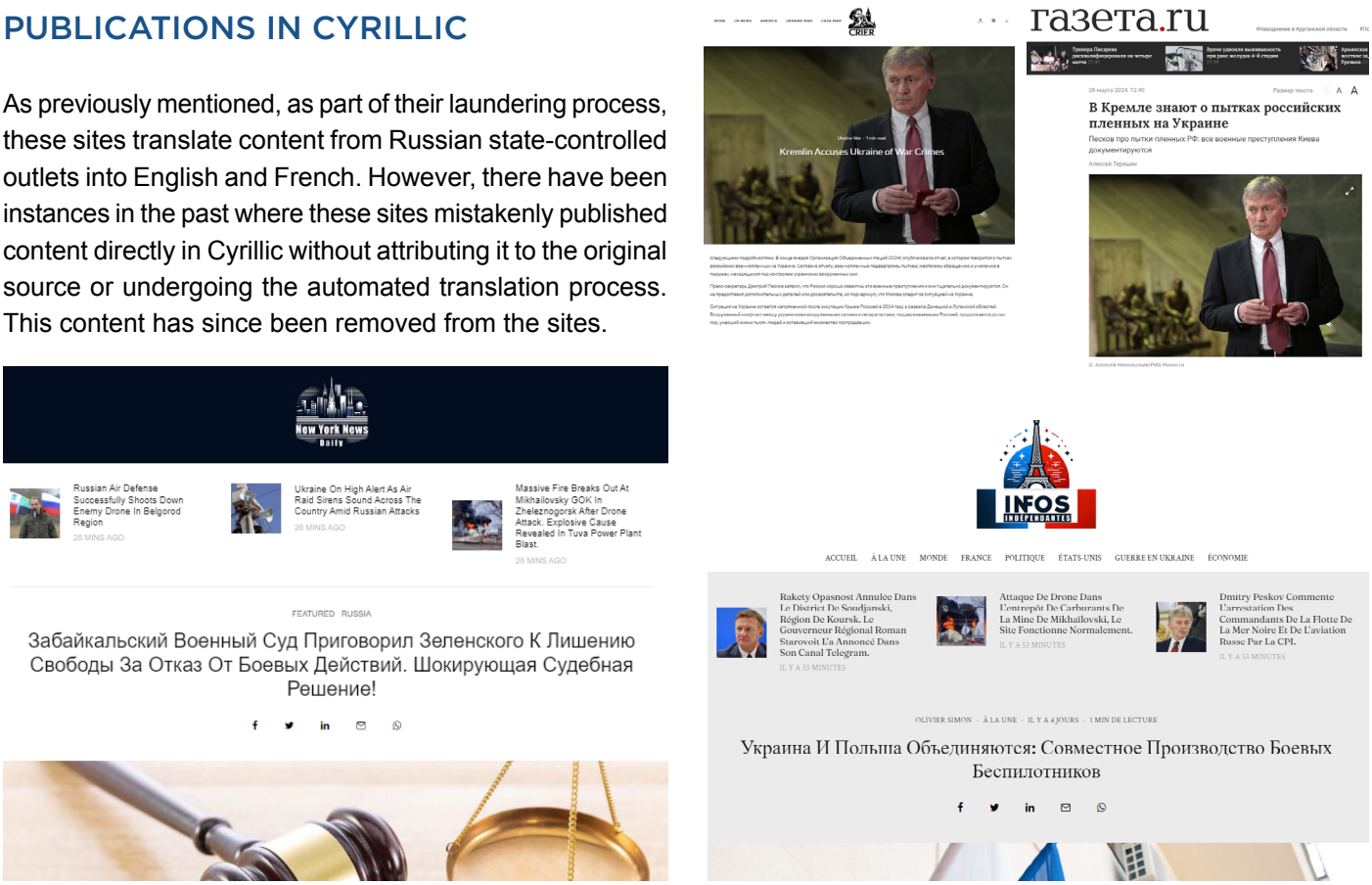


Figure 7: Screenshot of an instance in Russian published in londoncrier[.]co.uk[7] identical to the text published in Gazeta[.]ru and instances of other extracts in Russian published by the network[8].

Furthermore, references to the file names directories of certain images published in the articles also seem to be stored in Cyrillic characters.[6]

TECHNICAL AND BEHAVIORAL INDICATORS THAT LEAD TO NETWORK OPERATED GEOGRAPHICALLY FROM RUSSIA

- **Technical indicator:** Use of Cyrillic alphabet. The website published copy/pasted content in Russian and the names of some of the pictures and files are written in Cyrillic
- **Technical indicator:** Some of the IP addresses are located in Russia and belong to the same registrant entity: AS25513 - ASN-MGTS-USPD - PJSC Moscow city telephone network, RU.
- **Behavioral indicator:** Republication of non-original content from Russian sources into English
- **Behavioral indicator:** Russian diplomatic accounts and Russia state-controlled media amplified the content of the network
- **Behavioral indicator:** Campaigns previously attributed to Russia amplify the content of this network
- **Behavioral indicator:** Non-attributed sources that interact heavily with the Russian ecosystem amplifies and translate the content.

ANNEX: LIST OF IDENTIFIED SITES IN THE "FALSE FAÇADE" NETWORK AND INDICATORS

	Tracker ID	Common file names	IP address and registered company	Creation date and servers	Same web template	Name style	Similar logos	Content in Russian
falconeye.tech				2023-06-25				
autoconfig.falconeye.tech				2023-06-25				
autodiscover.falconeye.tech				2023-06-25				
info.falconeye.tech				2023-06-25	Ace News by Ascendoor			
monitor.falconeye.tech			95.165.88.254	2023-06-25	Ace News by Ascendoor			
www.falconeye.tech				2023-06-25				
dcweekly.org				2021-04-23	Zeen by Codetipi			
news.dcweekly.org			95.165.88.254	2021-04-24				
clearstory.news				2023-10-13	Zeen by Codetipi			
nynewsdaily.org				2024-01-18	Zeen by Codetipi			
infosindependants.fr				2024-01-27	Zeen by Codetipi			
miamichron.com				2024-02-26	Zeen by Codetipi			
londoncrier.co.uk				2024-03-26	Zeen by Codetipi			
chicagocrier.com			95.165.66.27	2024-03-17	Zeen by Codetipi			
sanfranchron.com			95.165.66.27	2024-03-17	Neonmagzin			
chicagochron.com				2024-01-06				
bostontimes.org			95.165.66.27	2024-01-18	Ace News by Ascendoor			
gbgeopolitics.com				2024-02-19	Newsmark			
londonchronicle.news				2024-02-19	Hello Elementor			
britishchronicle.com				2024-02-19	Zeen by Codetipi			
Londoncrier.com			95.165.66.27	2024-03-23	Zeen by Codetipi			
vidvist.com			95.165.66.27	2024-03-30				
disc.xposedem.com			95.165.66.27	2024-04-03				

REFERENCES

1 https://blogs.microsoft.com/on-the-issues/2024/04/17/russia-us-election-interference-deepfakes-ai/
2 https://www.sgdsn.gouv.fr/publications/portal-kombat-un-reseau-structure-et-coordonne-de-propagande-prorusse
3 More in NATO Strategic Communications Centre of Excellence, Information Laundering in Germany, 2020: https://stratcomcoe.org/cuploads/pfiles/nato_stratcom_coe_information_laundering_in_germany_final_web.pdf and James Pamment, Howard Nothhaft, Henrik Agardh-Twetman, and Alicia Fjällhed, Countering Information Influence Activities, Swedish Civil Contingencies Agency (MSB), 2018.
4 https://www.dw.com/en/fact-check-did-zelenskyy-buy-king-charles-highgrove-house/a-68777844
https://www.thejournal.ie/ukraine-zelenskyy-british-royal-residence-charles-iii-highgrove-estate-duchy-h-6356295-Apr2024/
https://www.ukrinform.net/rubric-factcheck/3848535-russian-propaganda-spreads-fake-about-zelenskys-purchase-of-royal-mansion-in-britain.html
5 https://archive.ph/B8QnG
6 https://archive.ph/qvWWi
7 https://archive.ph/iJ5b2
8 https://archive.ph/yLa0n


European Union
EXTERNAL ACTION