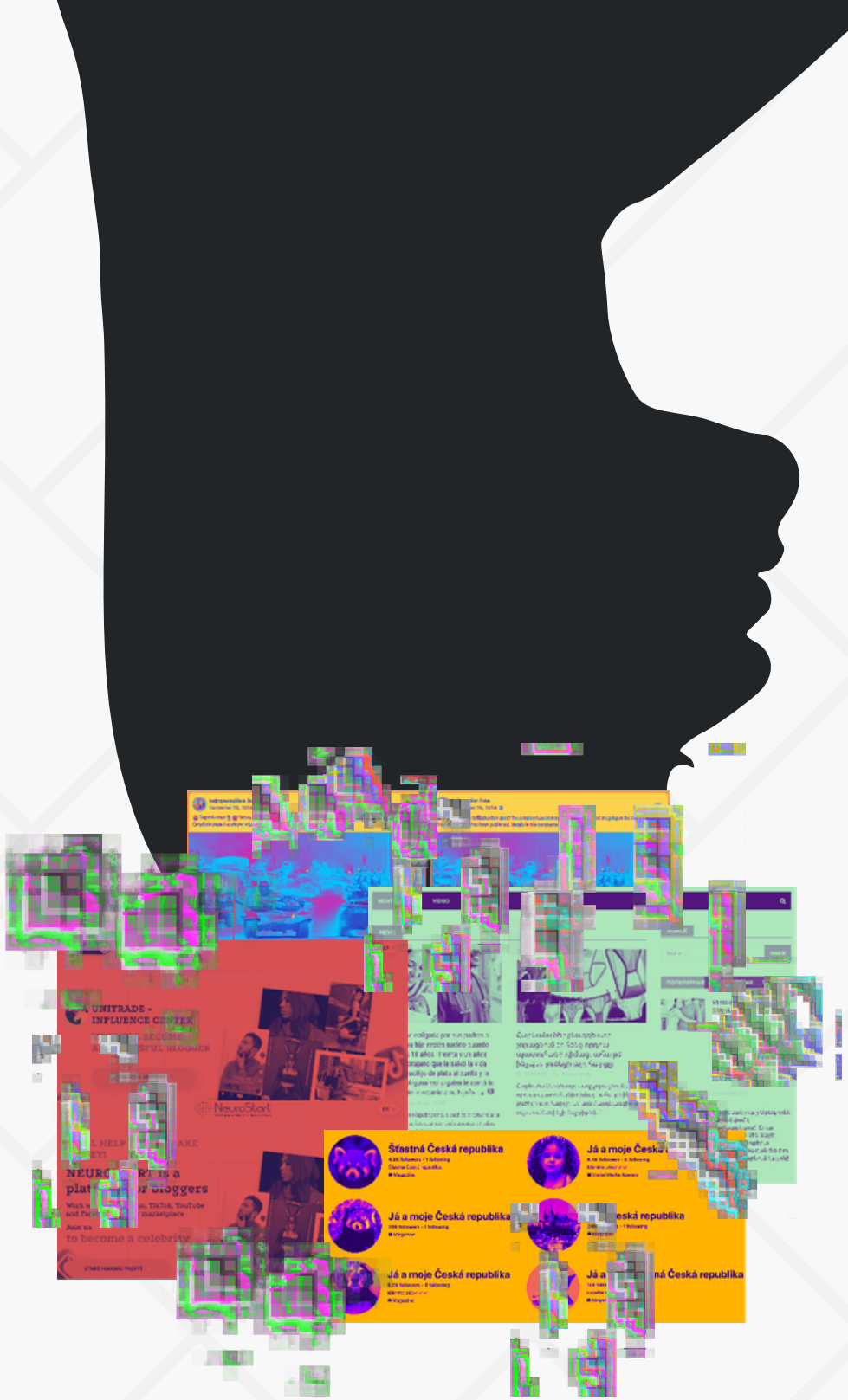


# Poisoning the Mind

Following ad revenue from deceptive websites to Russia's ruling party.

CHECK FIRST

# Poisoning the Mind

## Following ad revenue from deceptive websites to Russia's ruling party

**Author:**

Valentin Châtelet, CheckFirst (FIN)

**Contributors:**

Hervé Letoqueux, CheckFirst (FIN), Victor Ilie, Snoop (RO), Inna Gadzynska, Texty (UA), Iurii Agafonov, Infocom (AM), Josef Šlerka, Investigace (CZ).

*This investigation was supported by a grant from Journalism Science Alliance.*

| Version | Date | Description |
|---|---|---|
| 1 | 26/11/2026 | Initial release. |

Special thanks to all reviewers of this report for their feedback and support.

© CheckFirst 2026

Published in November 2026 under the **CC BY-SA** license.

# Table of contents


Executive summary....4
Key findings....5
Introduction....6
Methodology....7
Profit-driven clientèle exploits social media platforms to maximize ad revenue....10
Romania-based profit-driven CIB networks cash in thanks to ad revenue, echo pro-Georgescu support....10
Romanii Nostri-linked profit-driven operation....10
Extra News-linked profit-driven operation....12
Armenia-based profit-driven CIB networks cash in through MGID, AdsKeeper, target European audiences....13
Armenia-based CIB network targets Ukraine, Poland, Czechia....13
AI-powered Armenia-based CIB networks target global audience, floods social media with slop....15
AdNow's programmatic ad auction data reveals links to wider Serebryanskaya network....19
AdNow's online infrastructure suggests support of scam operations, exposes Novosibirsk defunct branch....20
Programmatic ad auctions data expose scam domains....20
AdNow reported defunct Novosibirsk branch hires freelancers to name scam products....21
AdNow defunct branch chief recruits freelancers to support United Russia candidate in election cycles....23
Serebryanskaya-linked initiative's IT infrastructure exposes links to European "influencer marketing agencies" and Ad[.]ru....25
IP address shares connections with "influencer marketing agencies" and other Serebryanskaya businesses....26
AdRu, AdNow and Fazze?....28
Conclusion....30
Appendices....31

## Executive summary

Between January and October 2026, a consortium of investigative journalists from Romania, Moldova, Czech Republic, Georgia, Armenia, Ukraine and the UK, together with CheckFirst, gathered advertising data in order to observe targeting strategies, narratives and money flows behind online disinformation campaigns and their potential links with Russian state actors. In particular, the experiment was designed to collect programmatic ad auction data with the aim of exposing advertising giants, and their role in supporting deceitful online actors. This research is based out of data collected by volunteers contacted by the consortium, who browsed the Internet using a CheckFirst web extension that intercepted web requests containing advertising information related to companies MGID, AdsKeeper and AdNow.

Our findings show that, out of the 45,931 transactions we captured using the CheckFirst web extension, the vast majority was imputable to more than 180 domains, that routinely publish clickbait, sensationalist AI-generated content. **This investigation illustrates how dark patterns exploited on social media and by advertising companies alike, have created a lucrative ecosystem enabling profit-driven enterprises to cash in.**

Furthermore, the campaigns designed by these profit-driven operators leverage social media amplification reaching millions of followers across Europe, and are aided by ad revenue strategies that seek to place deceitful and misinformed ads, often linking to scams, fake health supplements or websites sharing slanderous headlines to drive engagement and entice users. Our research mainly identified networks focusing on Romania, Ukraine, Czechia and Poland, as well as Armenia, where various deceitful online actors have deployed these campaigns since 2022 and the full-scale invasion of Ukraine by Russia.

Our research also uncovered AdNow-linked online infrastructure and historical data. AdNow, whose involvement in spreading anti-vaccine disinformation and sharing dubious links to pro-Georgescu information environment has already been largely reported on, further blurs the lines between the deceitful practices of its clients and its own role as a demand side platform. Our findings highlights that the company routinely hired freelancers to design campaigns promoting nutraceutical products as well as supporting the electoral campaign of the current Kaliningrad governor, Alexei Besprozvannykh. It also promoted offer domains that served more scams, and fake news sites' content. Links with AdNow founder, Yulia Serebryanskaya, also point to two influencer marketing agencies targeting Europe.

## Key findings

- 45,931 ad placement transactions collected by volunteers of the consortium using a CheckFirst web extension led to the identification of nearly 180 domains, believed to be associated with CIB networks operating on social media platforms, particularly on Meta.
- 92 domains link to at least six CIB networks operating fraudulent WordPress-powered blogs posing as news sites, and generating revenue by placing ads, targeting targeted Romania, Ukraine, Czechia, Poland, and Armenia.
- At least 34 inauthentic Facebook pages, were used by the network to entice users into clicking on sensationalist and click-bait posts
- Former AdNow director in Novosibirsk and other staff members used Russian platform FL[.]ru to share job postings to recruit freelancers to name and promote nutraceutical products, fake medicine and lander pages.
- AdNow's online infrastructure also shows connections to offer domains, reportedly flagged for phishing and scams, and also pose as fraudulent news blogs.
- AdNow and Serebryanskaya-linked business Tech47 share links to domains used for the 2024 campaign of United Russia candidate for Governor in Kaliningrad, Alexei Besprozvannykh, under international sanctions.
- Serebryanskaya-owned businesses "Russian Initiative" and "Asset Managment" share IP addresses with influencer marketing agency Neurostart.
- Serebryanskaya-owned online assets reveal historical IP address details linking to domain ad[.]ru and fazze[.]com.

## Introduction

This investigation draws upon data collected over a ten-month period by a consortium of investigative journalists, among which Snoop, Texty.org.ua, Investigace, Infocom.am and the Insider. Building upon previous publications which highlighted how Romanian citizens' data was harvested by advertising networks, this investigation reveals the tracking methodologies that have enabled us to capture advertising auctions data and identify deceitful online social media campaigns.

The premise for this investigation relied upon previous investigations that exposed how AdNow was involved in disinformation campaigns targeting French and German influencers to spread anti-vaccine narratives during the COVID-19 pandemic [1] [2] [3]. This investigation also draws upon the suspicions surrounding AdNow's leadership and closeness with Russia's ruling party, United Russia. Our intuition was to follow the trail of the leadership and Yulia Serebryanskaya-linked businesses, which enabled us to better map the ecosystem of her enterprises and how AdNow operates.

Additionally, Snoop's revelations showed that AdNow reportedly transferred nearly 2 million euros in total to several Romanian pro-Kremlin outlets, including the TV channel Romania TV. Together with multiple online campaigns that sought to push pro-Russian presidential candidate Călin Georgescu, we believed that advertising companies' roles in supporting enterprises of deceitful actors and disinformation constituted a legitimate motive for further investigation.

To that end, CheckFirst designed a web extension that intercepts web requests reaching out to advertising companies MGID, AdsKeeper and AdNow. By intercepting web requests sent to advertising companies' servers, CheckFirst was able to reverse engineer tracking mechanisms that contained Base-64 encrypted data, identifying how advertisers choose which ads to place, the cost of a programmatic ad auction and details about the advertising company. Once volunteers were equipped with the web extension, we analyzed the intercepted traffic and decoded the information that advertising companies collected using tracking pixels, which enabled us to further identify deceitful online practices.

Based on the retrieved data, we identified domains linked to phishing and scam operations placed by advertising company AdNow as well as other dormant domains, which pose as fraudulent WordPress-powered news sites to deliver ads. This further enabled us to probe the infrastructure of lucrative campaigns and how they rely upon ad revenue to sustain themselves and how social media platforms, particularly Meta, have become an unavoidable breeding ground for these dark patterns to take root.

## Methodology

In December 2025, CheckFirst developed a web extension to collect programmatic ads placed by advertising companies to users browsing the Internet. The aim of our investigation was to expose the role of advertising company giants including AdNow, MGID and AdsKeeper in placing targeted ad campaigns online, and how they enabled or took part in deceitful, scam and disinformation enterprises. In addition to gathering the data related to programmatic ad auctions, we investigated the underlying web infrastructure operated by advertising companies and their clients to understand how it intended to increase ad revenue by enticing users using fake social media assets.

The experiment was conducted during a ten-month window between January and October 2026, capturing 45,931 transactions placing 62,148 ads auctioned by the advertising companies laid out above across 1,776 web pages. The data was collected thanks to civil society volunteers who agreed to install the extension and browsed the Internet, including suspicious online assets that exhibited traits of fraudulent content, to organically collect the placed ads. The data we collected using the web extension also contained payloads recording the transactions resulting in the ad placement as well as the redirection loops between known advertising companies' domains and other servers responsible for the ad auctions.




*Figure 1. A donut chart showing the distribution of the 45,931 captures across the three advertising networks. (See Appendix. 3)*

CheckFirst's web extension was designed to intercept web requests reaching advertising companies' domains when ads are placed on a website. The premise laying the groundwork for this study posited that, by collecting this data, one could map out the ecosystem of the advertising companies' online infrastructure, their clientèle and the type of ads served depending on the website that was browsed.

We first identified domains used by advertising companies by leveraging the sellers.json file data. This file is placed by advertising and marketing companies at the root of their websites and lists the ad exchange and supply-side platforms acting as middlemen for programmatic ad auctions. These are often domains used by advertising companies, with the purpose of not only serving the auctioned ads, but also to track auctions and record transactions.

### Programmatic ad auctions

Advertising platforms act as a market place connecting sellers and buyers to place ads on websites. Upon browsing the web page of an advertising platform client, a programmatic ad auction will determine which ad to place on the website. The section dedicated to ads on the web page is called an "opportunity." Sellers are advertising platforms' clients who offer sections of their websites for ad placement. Sellers provide opportunities, while these are auctioned by the advertising company, that acts as a middleman, and sold to a buyer, i.e. an advertising platform client whose content will be placed as an ad on the seller's web page. The result of this transaction is what is in broad strokes referred to as a programmatic ad auction.

Advertising platforms execute auctions in the background when users browse sellers' websites to determine whose ad should be placed on their web page, i.e. which buyer should benefit from the opportunity to place their content. Buyers' ads bid on the given opportunity; winning the auction depends on multiple factors, such as location or branding.

By reverse engineering the API endpoints queried by the advertising companies' scripts embedded their clients' websites, we collected ad responses, and encrypted payload data, that record transactions of the ad auction resulting in the ad placement. The transaction record of the programmatic ad auctions is saved as a Base-64 encoded string, embedded in the URL of tracking pixels—images used by advertising companies to identify client websites and sellers and track customers online.

### Tracking pixels and auction data

According to Cookiebot, a tracking pixel is an invisible 1x1 image or line of HTML code embedded in websites, emails, or digital ads that silently pings a server to record user interactions. In emails, tracking pixels can inform senders whenever an email is opened by the recipient. For advertising and web tracking purposes, tracking pixels encode information about users, including their location, UI interactions, duration of visit and IP addresses.

During the development of the web extension, CheckFirst identified that tracking pixels featured a GET request parameter that contained a Base-64 encoded string in the URL. For advertising companies that used this tracking techniques; this enabled us to retrieve auction and transaction information such as:

- CPA (Cost per Action): online ads measurement and pricing models for actions (click, form submission...).
- DSP (Demand Side Platform) prices: Prices determined by automated systems used by advertising platforms to buy and sell impressions
- Bids and prices for placed ads.
- Domains used by advertising companies to serve ads.
- Email addresses used to record transactions.

Using this information, we narrowed down the list of domains we obtained by browsing the Internet over ten months, to focus on the main advertising companies and clients who seemingly generated significant ad revenue based on the tracking pixel decoded data.

## Profit-driven clientèle exploits social media platforms to maximize ad revenue

The findings of this experiment identified more than 180 fake news sites, that generate advertising revenue using AdNow, MGID and AdsKeeper. The data we collected also highlights that, by far, these sites are part of multiple networks orchestrated by deceitful online actors that have designed profit-driven coordinated inauthentic behaviour (CIB) operations. These operations rely on posting sensationalist, fringe or fake stories and using AI to automate content generation while disseminating it on social media platforms, particularly on Meta. In addition, leveraged advertisement revenue through AdNow, AdsKeeper and MGID, may in reality sustain wider profit-driven information manipulation sets (IMS) driven by deceitful actors, and further advertise scams.

More generally, individual or smaller size enterprises also intended to generate ad revenue using inauthentic social media assets, a tactic observed no matter how big the profit-driven enterprise was, in order to drive traffic to fake sites. Our investigation explores four networks of profit-driven inauthentic content generation factories that comprised Facebook pages and fake sites, showcasing the strategies of profit-driven deceitful actors. These actors targeted audiences in Ukraine, Romania, Armenia, Czechia, and Poland and operate dozens of online assets, which may be tied to hundreds of prior assets that are now inactive.

Our work not only exposes the deceitful practices of advertising companies' opportunity sellers, but also questions said companies responsibilities in monetizing fraudulent online enterprises and tracking customers' data. According to Snoop and Romania's National Authority for Management and Regulation in Communications (ANCOM), profit-driven fringe Facebook pages and false information news sites have widely benefited from AdNow's revenue system. As reported by Texty.org.ua, by engaging in posting sensationalist, fringe or even content users landed on fraudulent WordPress-powered news sites promoting fake medicine and disinformation. This trend notably exacerbates how social media users may be targeted by deceitful advertising practices and fake online content.

## Romania-based profit-driven CIB networks cash in thanks to ad revenue, echo pro-Georgescu support

### Romanii Nostri-linked profit-driven operation

Together with the Romanian outlet Snoop, CheckFirst established that the fringe news outlet RomaniiNostri[.]ro harvested Romanian users data and cashed in on ad revenue using ads placed by Russian company AdNow. Our findings indicate that RomaniiNostri[.]ro's digital footprint encompasses at least four fake sites posing as news blogs active between 2022 and 2026. Each site was also linked to a network comprising at least thirteen inauthentic Facebook pages reposting content, sharing the original material hosted on the fake site.

Multiple fake sites also generated ad revenue through AdNow and AdsKeeper. These were first exposed in a June 2026 Facebook post by Romania's Minister of Investments and European Projects and interim Minister of Labor, Dragoș Pîslaru. Additionally, Pîslaru accused 42 Facebook pages in the network — most of which were still active at the time of writing this investigation — of being "a premeditated disinformation operation" and that they had reportedly "[...] been used in recent weeks in a coordinated campaign of manipulation designed to induce panic and revolt around the draft unitary pay bill ". These linked to RomaniiNostri[.]ro and other affiliated fake news sites.

By using reverse tracker and ad codes, we found that RomaniiNostri[.]ro was in reality linked to at least three other fake news sites, that engaged in publishing sensationalist content and misinformation together with AI-generated stories and visuals.

| Domain | Google Tag |
|---|---|
| ziarulzilei[.]net | pub-4744342340160921 |
| stiriglobale[.]ro | pub-4744342340160921 |
| darulnostru[.]ro | pub-4744342340160921 |
| romaniinostri[.]ro | pub-4744342340160921 |

*Figure 2. Four inauthentic fake WordPress news sites sharing a Google AdSense code.*

We identified a network of at least thirteen Facebook pages totaling 3.4 million followers that systematically reposted content linking to the four sites cited above. Only three of these pages had been mentioned in Pîslaru's post, highlighting that the network is still at large and wider than anticipated. (See Appendix 4.)

In multiple instances, we observed that network amplified news posted by pro-Russian news outlet *Romania TV*, one of several media outlets that reportedly received a combined total of nearly two million euros through AdNow between 2016 and 2020. The below posts notably show how a story about a declaration by Georgescu's spouse originally posted by *Romania TV* was amplified by the network .



*Figure 3. Three posts amplifying a* Romania TV *story about Cristela Georgescu. (Source: MOOD, Tezaur de Curiozități, Omul cu Sulfet)*

## Extra News-linked profit-driven operation

In addition, Pîslaru also exposed the fraudulent news site ExtraNews[.]ro. Similarly to the network laid out above, we identified at least six Romania-focused fake sites operating as news outlets since 2016 that are connected to ExtraNews[.]ro. Our findings confirm that this network benefited from ad revenue generated using AdsKeeper and MGID. In total ExtraNews[.]ro is likely connected to a web of thirteen fake sites that have been active since late 2016. Our findings indicate that at least ten websites have shared an identical Google AdSense code use by ExtranNews[.]ro, two of which were registered out of Russia in 2016. According to Builtwith.com, ExtraNews[.]ro also shared an MGID tracking code with an additional three websites between 2020 and 2024.

| Domain | Google Tag |
|---|---|
| g2g[.]ro | pub-4576701718373348 |
| cyd[.]ro | pub-4576701718373348 |
| matinalromania[.]ro | pub-4576701718373348 |
| adevaruldeazi[.]ro | pub-4576701718373348 |
| romaniamatinal[.]ro | pub-4576701718373348 |
| news-zone[.]ro | pub-4576701718373348 |
| realitateadeazi[.]ro | pub-4576701718373348 |
| likes-news[.]info | pub-4576701718373348 |
| likes-news[.]ru | pub-4576701718373348 |

*Figure 4. Ten sites that shared* extranews[.]ro *Google AdSense code.*

Furthermore, on Facebook, assets that reposted Extra News' content often obfuscate links to the source material using link shortener service Cutt.ly. We found a network of at least nine Facebook pages totaling 4.8 million followers, three of which were initially exposed by Pîslaru, that also took part in the systematic dissemination of the content posted on the websites listed above. (See Appendix 5.)

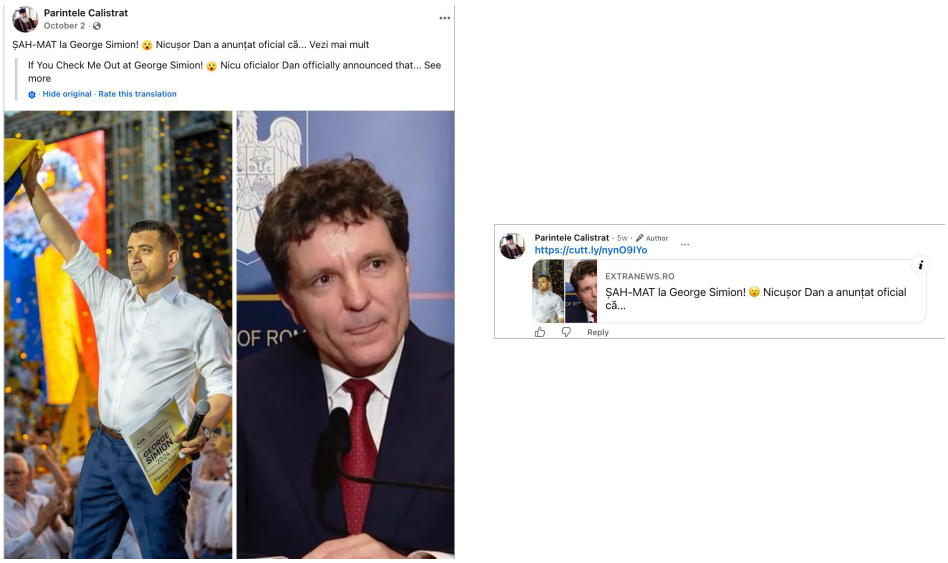


*Figure 5. A sensationalist Facebook post with photos of Romania's President Nicușor Dan and former presidential candidate George Simion linking to extranews[.]ro using link shortening service cutt.ly. (Source: Parintele Calistrat)*

## Armenia-based profit-driven CIB networks cash in through MGID, AdsKeeper, target European audiences

In addition, our findings exposed at least two inauthentic profit-driven CIB networks that leverage networks of dozens of fake sites and social media assets reportedly based out of Armenia with a focus on foreign audiences. Our analysis also highlights that these actors have a long standing history spanning over a decade of exploiting social media vulnerabilities and advertising revenue, by first targeting domestic and then foreign audiences.

### Armenia-based CIB network targets Ukraine, Poland, Czechia

The collected data highlights that one network in particular, comprising at least thirty-two fake sites posing as news blogs, has been active in the wake or shortly after the beginning of Russia's full-scale invasion of Ukraine in February 2022. This network first focused on spreading sensationalist and misleading stories about the ongoing war, using inauthentic Facebook pages that first targeted Ukraine, and gradually expanded to also encompass Polish and Czech audiences.

Our research first identified the domains bestzone24.biz[.]ua and dailytimes.biz[.]ua, both mentioned by a network of inauthentic Facebook pages. The collected data shows that these generated ad revenue through MGID. By investigating the inauthentic Facebook pages the operators used for content dissemination, we identified thirty-one additional domains that belonged in the network and shared at least three common MGID tags [1] [2] [3] according to Builtwith data. (See Appendix 7.)

The Builtwith records also show that some domains were activated using a single MGID code throughout August 2026 every three days, hinting at signs of automated deployment.

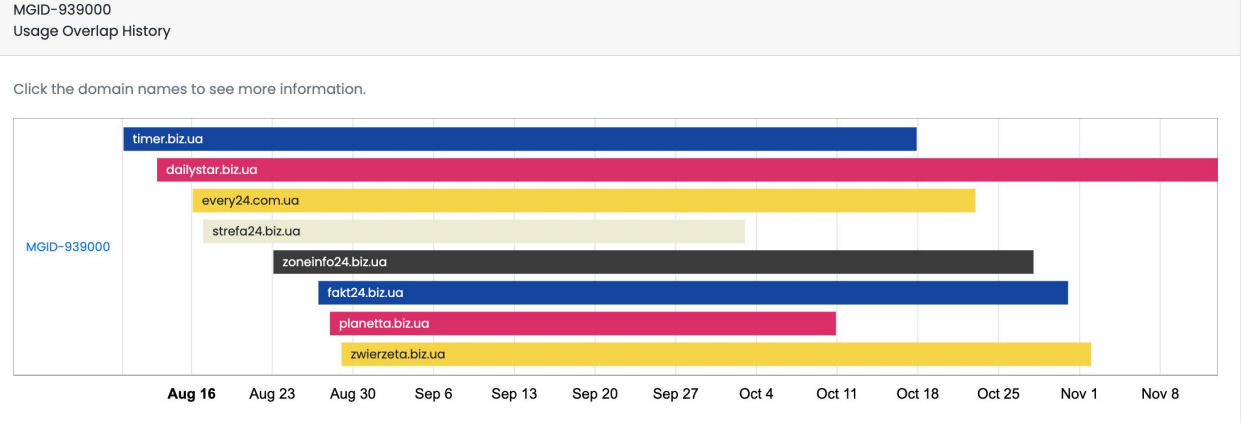


*Figure 6. A Builtwith horizontal bar chart showing the first records of activation of the MGID tag on the websites identified within the network. (Source: Builtwith)*

At its core, the network established various Ukraine-focused inauthentic Facebook pages tied to an Armenia-based operator, that sought to monetize fake and sensationalist content related to the war. This network was also reported on by Ukrainian media outlet Texty.org.ua, for its publishing of health related scams on the websites linked to the Facebook assets.

At the time of writing, although the content disseminated exhibits obvious traits of AI-generation, the Facebook pages created in 2022 spread stories about the war in Ukraine, and used algospeak to further obfuscate the deceitful nature of the disseminated content. We found that the pages spread sensationalist and misleading narratives exaggerating Russian gains and Ukrainian losses on the battlefield, false claims about the mobilization in Ukraine, and attributed incomplete statements to politicians and public figures. The use of algospeak — replacing conventional letters by other similar looking Unicode symbols — most likely attempted to evade content moderation and, ultimately, deplatforming.



*Figure 7. A Facebook post (at left) translated using Google (at right) that amplifies misleading narratives about Russian gains in the war in Ukraine, using algospeak to likely evade content moderation. (Source: Facebook)*

Gradually, the network expanded to include pages that launder its content in Polish and Czech. According to Facebook's transparency data, the pages all reported their locations as "Armenia." Although this information was not independently verified, we noticed that the page Zvistka was following Armenian page titled "Սամվել Բաբայան ֆան/Samvel Babayan Fan," while page "Непереможний народ" (Invincible people) also followed a French-language page about the Armenian Diaspora.[1]

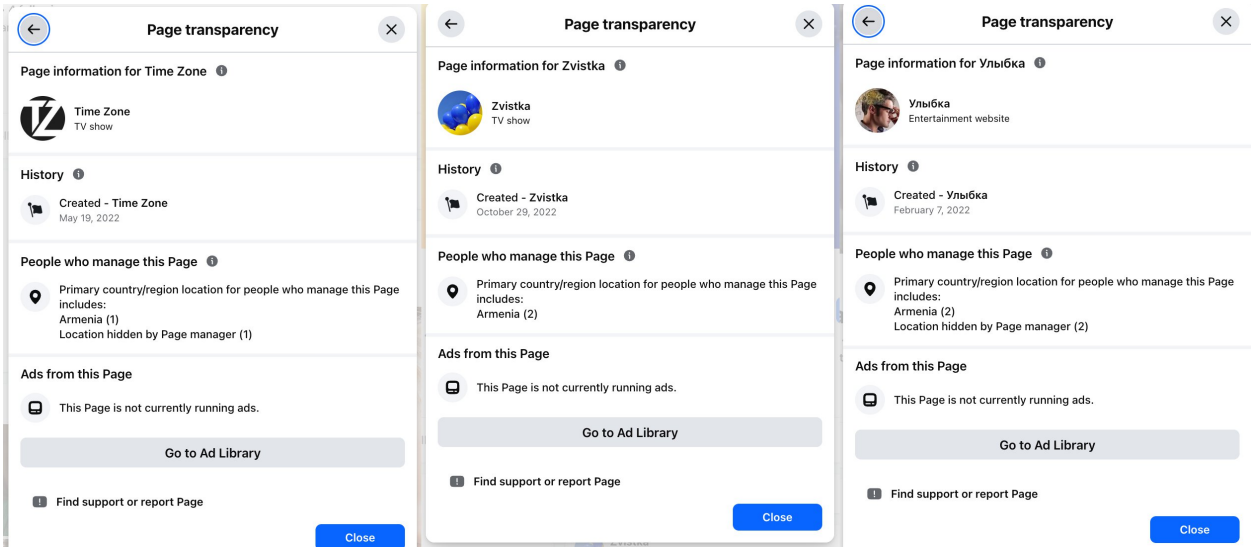


*Figure 8. A comparison of three Facebook pages in the network all showing "Armenia" as the reported location of the operator(s). (Sources: Time Zone, Zvitka, Улыбка)*

The Polish and Czech pages also posted political content with a sensationalist flair. For instance, two coordinated Czech pages posted a story [1] [2] that inquired about the consequences of Russia's proposed peace deal including the removal of NATO troops from most Eastern European countries on the sidelines of the current meeting between belligerents in Abu Dhabi, and argued about the potential consequences for Czechia.

## AI-powered Armenia-based CIB networks target global audience, floods social media with slop

In October 2024, Armenian news outlet Hraparak.am exposed fraudulent news site hraparaknews[.]am, a domain typosquatting the legitimate news organisation. The fraudulent news site, along four others have reportedly published fake or sensationalist news stories about extreme weather, often attributing false statements to official institutions in the country. Our research shows, that the network comprises in reality ten active domains, all hosted on IP address

[1] In addition, another Armenia-based network targeting audiences in Ukraine comprised of multiple pages, that authored reviews on an Armenian Health Center.

95.142.40[.]92 registered out of Russia. Additionally, these sites all use AdsKeeper to generate ad revenue, and drive traffic by using inauthentic Facebook pages.

| Domains | IP |
|---|---|
| chex[.]am | 95.142.40[.]92 |
| chexia[.]info | 95.142.40[.]92 |
| chxial[.]am | 95.142.40[.]92 |
| filan[.]am | 95.142.40[.]92 |
| gazeta[.]am | 95.142.40[.]92 |
| hayreniq[.]am | 95.142.40[.]92 |
| ital[.]am | 95.142.40[.]92 |
| usmedtrade[.]com | 95.142.40[.]92 |
| vengria[.]info | 95.142.40[.]92 |
| vendeto[.]am | 95.142.40[.]92 |
| hraparaknews[.]am | 95.142.40[.]92 |

*Figure 9. A table of the domains hosted on IP address 95.142.40[.]92*

The network has been active since at least 2023 and encompasses a staggering 27 domains registered since then. (See Appendix 6.) It registered typosquatted domains to entice and mislead users to their news stories. For example, since 2024, the network has used the domains gazeta[.]am, bbcnews[.]am, and kommersant[.]am typosquatting legitimate international and Russian-language media outlets.

Over the years, the network grew exponentially, and delegated much of its content generation to AI systems and LLMs reaching a wider global audience. A cached Google search result from September 2026 notably indicates that the domain harcum[.]am used an LLM to generate stories in English. Facebook pages associated with the network also routinely post AI-generated reels.

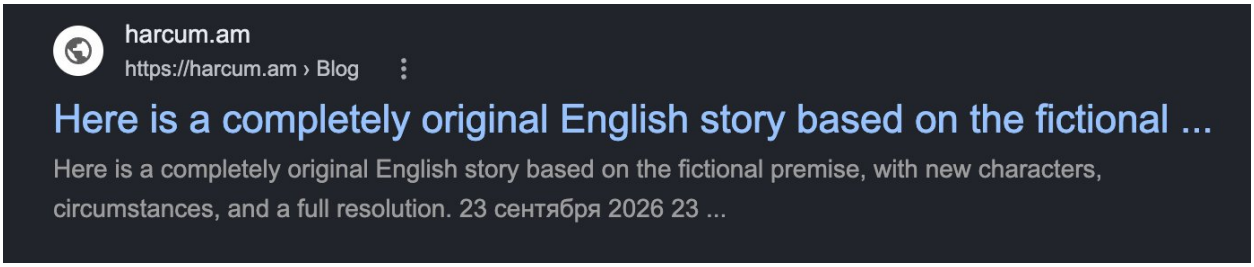


*Figure 10. A screen capture of a Google search for domain harcum[.]am shows the opening line of an LLM response.*

However, the latest ten active domains seem to have shifted from the typosquatting strategy. By analyzing the content published by vendeto[.]am, we found that the newest iteration of this profit-driven operation published content in a variety of languages, including Czech, Hungarian, English, and Spanish regardless of the domain name. The WordPress language configuration of the fake sites however, remains Russian.

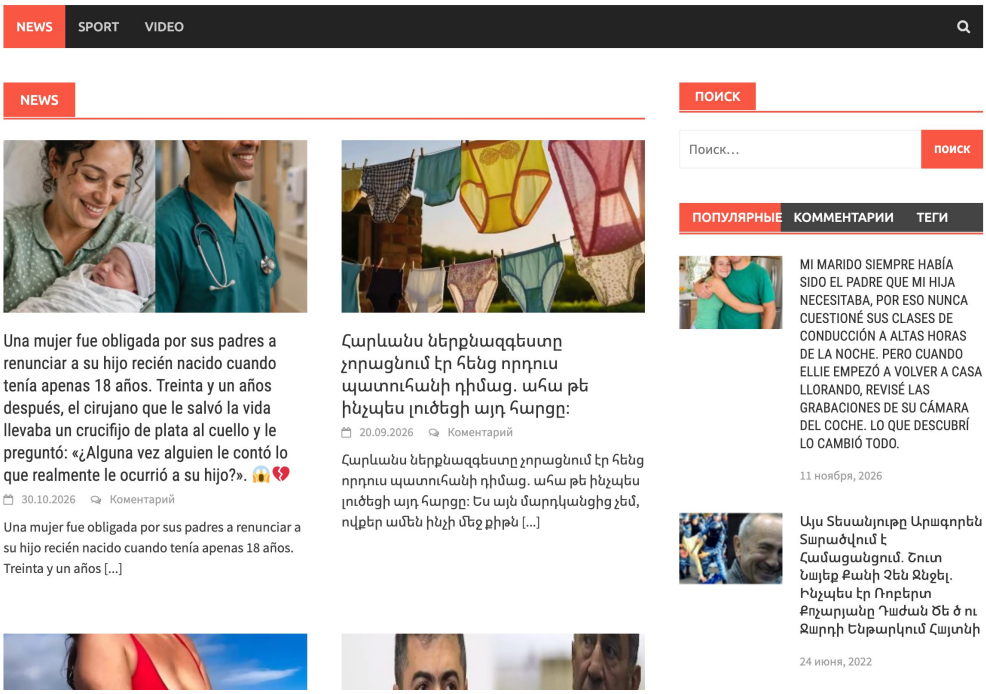


*Figure 11. The homepage of fake site vendeto[.]am showing UI in English and Russian, articles in Spanish and Armenian. (Source: vendeto[.]am)*

The Czech language posts were also systematically amplified using inauthentic Facebook pages, with patriotic-sounding names such as "My homeland," "Happy Czech Republic," "Me and my Czech Republic," and "Interesting stories in the Czech Republic ". In total, we found ten inauthentic Facebook pages that had amassed 134.6 thousand followers, also targeting audiences in Hungary and Spain republishing content from the fake sites. (See Appendix 8.)




*Figure 11. Six inauthentic Facebook pages part of the network targeting Czechia. (Source: Facebook)*

Some of these Facebook pages that historically posted content linking to the above domains, have recently started publishing links to arminfonews[.]ru and very-amazing[.]com, two websites that

link to yet another Armenia-based network of fifteen other fake sites, that have been active since 2020 according to Builtwith data. This underscores that the networks we investigated, may encompass more countries and that they have likely been sustained primarily thanks to ad revenue, and that operators likely resell Facebook assets. A third Armenia-based network we identified, operates twelve fake sites, all amplified using CIB via Facebook pages. These all shared an identical Google Ad Sense code and generated revenue through MGID.

| Domain | AdSense code |
|---|---|
| newlike-info[.]ru | pub-5969530888515309 |
| info-cool[.]ru | pub-5969530888515309 |
| armcool[.]ru | pub-5969530888515309 |
| like-cool[.]ru | pub-5969530888515309 |
| cool-like[.]ru | pub-5969530888515309 |
| like-info[.]ru | pub-5969530888515309 |
| like-cool[.]online | pub-5969530888515309 |
| newlike-info[.]online | pub-5969530888515309 |
| natureagreable[.]com | pub-5969530888515309 |
| interesinfo[.]ru | pub-5969530888515309 |
| amazingpage[.]ru | pub-5969530888515309 |
| likenews-info[.]ru | pub-5969530888515309 |
| newsarm-info[.]ru | pub-5969530888515309 |

*Figure 12. Arminfonews[.]ru linked domains sharing a Google AdSense code.*

While most of the Facebook pages associated with the network have either gone silent or republish AI-generated stories, this trend reveals that for-profit CIB operations can be deployed to target a variety of audiences in multiple languages and that despite the deceitful nature of the content they create, operators of these networks generate ad revenue *en masse* by abusing social media assets and, in all likelihood, automating the deployment of the fake sites used throughout their influence campaigns.

## AdNow's programmatic ad auction data reveals links to wider Serebryanskaya network

We coupled this data-driven approach to a deeper investigation of the web infrastructure of Russian advertising company giant AdNow, due to its prior implication in disinformation campaigns targeting Europe and particularly Romania. As a reminder, in 2021, Meta and Meduza exposed how the UK-registered marketing firm Fazze placed deceitful Facebook ads and reached out to influencers in order to spread misinformation and false anti-vaccine narratives during the COVID-19 pandemic. According to Meduza, Fazze was linked to the Moscow-based advertising company AdNow created by Yulia Serebryanskaya, a former PR aid to the campaigns of presidents Dmitri Medvedev and Vladimir Putin.

### The Serebryanskaya galaxy

Yulia Serebryanskaya is a Russian entrepreneur who reportedly owned AdNow's Russian branch until 2018. According to Russian online outlet FedPres[.]ru, in 2012, Serebyranskaya founded the IT marketing company 2WTrade, which also had a London-based subsidiary she owned until 2016. The company reportedly sold beauty and health items. According to RFE/RL mentioning an internal document with a flow chart, Serebryanskaya's marketing company 2WTrade shared links and a postal address with AdNow in Moscow.

FedPress indicates that since 2003 Serebyranskaya held various positions working for state-funded Russian media such as NTV, where she reportedly "prepared a series of programmes about the life of the Russian population of Ukraine ". In 2007, Serebryanskaya reportedly worked for the presidential campaign of Dmitry Medvedev, where she was "responsible for 'video clips' for the candidate ". That same year Serebryanskaya reportedly also produced video material in support of Vladimir Putin. In 2008, she reportedly "took part in the development of ads for Russia's Central Electoral Committee," and was appointed "deputy head of the management of the [United Russia]'s Internet projects ".

In addition, following the 2024 annulment by Romania's Constitutional Court of the first round of the presidential election over concerns of foreign interference, Romanian investigative news outlet Snoop uncovered that AdNow transferred nearly two million euros to pro-Kremlin TV stations in the country. Reportedly, AdNow also used Facebook again to spread pro-Georgescu messaging using fraudulent pages advertising for alternative medicine and scams. The then pro-Russian front-runner and former presidential candidate Călin Georgescu was detained in September 2026.

Our investigation shows that AdNow in reality shares linkages with multiple advertising, marketing and tech companies within the Serebryanskaya galaxy. By analyzing the ad auctions payload data, we identified former and current employees linked to AdNow's now defunct Novosibirsk subsidiary and their campaigns in support of a candidate from Russia's ruling party, United Russia.

## AdNow's online infrastructure suggests support of scam operations, exposes Novosibirsk defunct branch

Throughout this investigation and thanks to the collected data, we have exposed how AdNow's ad revenue system blurs the lines between clients and providers. By analyzing the ad auctions' data contained tracking pixels' URLs, we've exposed how AdNow linked to offer domains that are effectively placing ads containing scams and health supplements advertised to social media audiences. We also found out that fake outlets used by inauthentic social media pages may share more than just a tracking code, and link to AdNow's IT infrastructure.

Our investigation also casts a serious doubt on whether the company itself partook in the creating and tailoring of "nutraceuticals ". Records linking staff members and former leadership indicate that they may well be involved in recruiting freelancers to design online campaigns targeting foreign audiences with fake medicine. These also strongly suggest that the lines between AdNow and other businesses in the Serebryanskaya galaxy, such as the "Russian Initiative," — a nationalist non-profit organisation promoting Russian patriotism — may be less salient than previously thought. Our investigation shows how AdNow Novosibirsk former leadership could be at the origin of dubious ad campaigns and may have provided United Russia candidate with IT and PR support.

### Programmatic ad auctions data expose scam domains

To collect programmatic ad auction data, we first mapped out AdNow's servers involved in serving and providing ads. As reported in Snoop's investigation, one of these servers nnowa[.]com was used to place such content—together with two subdomains ("n", "st" or "st-n") that are used for ad delivery and tracking—. This subdomain structure was also shared across all AdNow domains we found that delivered ads on IP address 31.172.81[.]226. (See Appendix 1. and 2.)

In addition, we identified twenty-three domains that shared name servers ns.gdnst[.]pro and gns.gdnst[.]pro which also featured the aforementioned subdomains "n" and "st." These characteristics are shared by nnowa[.]com and other official AdNow domains. Although we only focused four of AdNow's domains in during our data collection, the remaining twenty domains are believed with very a high level of certainty to be associated with AdNow infrastructure. (See Appendix 9.)

By analyzing 17,368 recorded ad auctions' encrypted data pointing to AdNow, we identified seven domains linked to the company. Most notably, these seven additional "offer" domains are used to place ad content. Multiple of these domains have been flagged as scams or phishing operations in a Poland's CERT Polska list and by the Phishing army. These include health scams, as well as financial scams, including neotex[.]pro and news360[.]pro.

| Offer domain | Occurrences | Captures | Distinct offer IDs |
|---|---|---|---|
| neotex[.]pro | 12762 | 3939 | 65 |
| news360[.]pro | 2354 | 691 | 28 |
| datanexpress[.]com | 1498 | 549 | 24 |
| 24news[.]life | 734 | 255 | 10 |
| neodilio[.]com | 8 | 4 | 1 |

| | | | |
|---|---|---|---|
| quorxalenth[.]info | 8 | 4 | 1 |
| zoomingheadlines[.]online | 4 | 2 | 1 |

*Figure 13. A table of offer domains linked by AdNow issued advertisement.*

The above domains share characteristics with AdNow's servers that cast doubt upon their actual ownership and links to the company. According to a November 2 publication by Ukrainian security company GridinSoft, the domains 24news[.]life and st-n.click116[.]com are linked to pixeldeliver[.]info, a Russian WordPress website, which they reported as a phishing domain, calling for its blacklisting. By collecting pixeldeliver[.]info's data, we also found that it operates as a fraudulent news outlet in dozens of languages, reposting news from legitimate sources, presenting them with clickbait headlines, with more than 10,730 articles published since the website's inception in January 2026. click116[.]com is further linked to AdNow due to their common use of the name server gdnst[.]pro. In addition, the aforementioned domain 24news[.]life operates as an offer domain linked by AdNow to place ads. Although pixeldeliver[.]info's true ownership remains unknown, this evidence strongly suggests that it may well be yet another iteration of a fraudulent news site, linked to AdNow's core infrastructure that is likely to generate ad revenue either by placements from the company or by being advertised for by inauthentic social media assets.

## AdNow reported defunct Novosibirsk branch hires freelancers to name scam products

The decoded payload data that was used to compile the domains identified above, also contained email addresses pointing to alleged staff member of AdNow. Our investigation shows that in particular, two employees have since 2010 used a Russian online platform to hire freelancers for copyrighting, web development and graphic design supporting AdNow's scam development operations for at least a decade.

Three email addresses belonging to two Russian individuals have led us to a trail of odd job postings on Russia's freelancer recruitment platform, FL[.]ru. The individuals are Novosibirsk-based Russian men, who went by usernames mixing references to advertising and abbreviations for Novosibirsk. In 2016, an FL account posted an ominous job ad for "copywriters" where contenders were invited to "tell engaging and captivating stories that present the benefits of a product in an unconventional way." In reality, the account's posting tasked copywriters with writing advertisement for three fake stories that promoted fake products including health treatment against varicose.

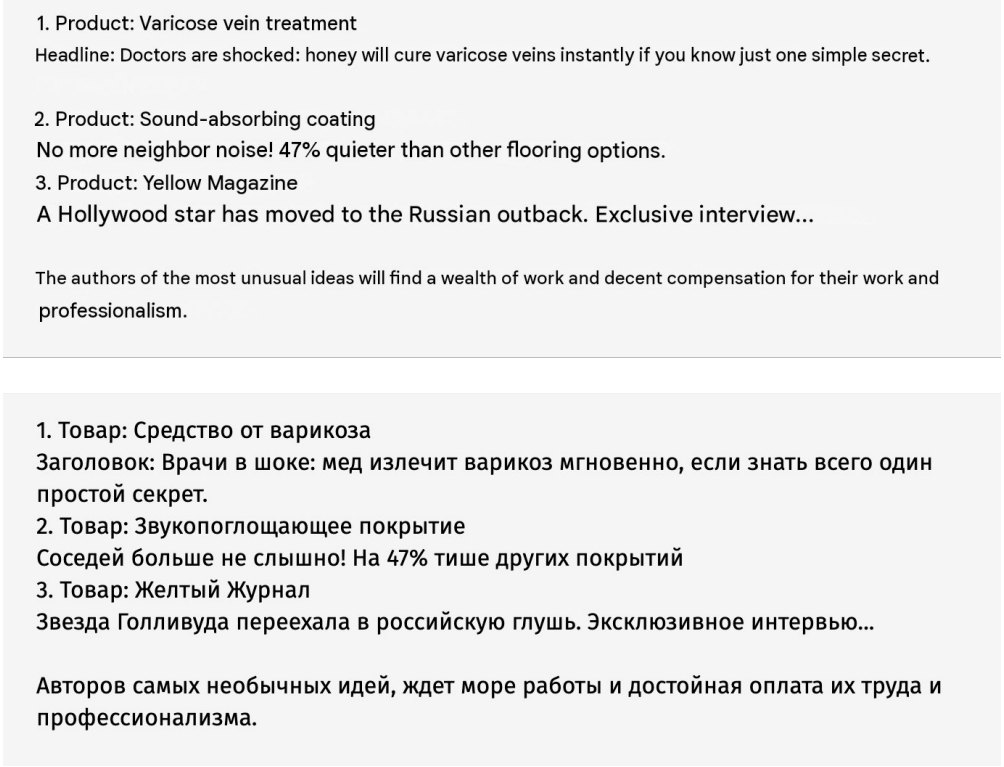


*Figure 14. A job ad description prompting copywriters to advertise fake products and sensationalist stories. Translation (top), and original (bottom). (Source: FL/archive)*

According to Russia's business register, AdNow opened a Novosibirsk branch in December 2016 under the name "EDNAU NSK," although prior reports indicate that AdNow started its activity in 2014. Coincidentally, we found that the former head of AdNow in Novosibirsk had also been recruiting freelancers via job postings on FL. Using email address adnow-web@yandex[.]ru, this account started to actively recruit for health and food supplement-related campaigns between 2019 and 2022, tasking freelancers with finding names to promote among others:

- "hair-vitamin gummies,"
- "a gel against joint pain,"
- "a brand name for a cold remedy,"
- "a product for the treatment and prevention of influenza and acute respiratory viral infections (ARVI),"
- "a brand for a line of pain-relief medications,"
- "a brand of household cleaning products,"
- "a remedy for PMS and dysmenorrhea,"
- "drops against parasites."

Almost across all postings, the author also mentioned "the name must be in English; do not use transcription" and indicated a target group, usually comprised of "women between 30-60 years old" — although one product "Shark Motion" also targeted men above 35 years old.

This strategy indicates that the author of the posts mostly focused on "Nutra vertical" affiliate marketing, where non-medical products are advertised to generate ad revenue. This is further illustrated by a 2023 job posting by the account that intended to recruit a freelancer to "Draft the text for a pre-lander" to write "between 7 to 9 pieces" about "nutra-vertical." The posting also indicates that the contender should have "experience in working with CPA-networks" and "experience in writing pre-landing and transit pages."

### Nutra-vertical or "nutraceutical" advertising

According to RichAds, nutra-vertical "(...) describe[s] offers that fall into a broad category of products for health and beauty. The term applies to the products there are mostly non-medicated substances, supplements and vitamins." The publisher also warns "notice that the general meaning of Nutra offers is that they are not conventional medicine. Such products are dispensed without a prescription, and the audience usually purchases them as an alternative to mainstream medicine care."

In its postings, however, the account clearly indicates that these "alternative medicines" should be considered competitors to "Ibuprofen" or "Ketoprofen" indicating that the authors intended to present these products as genuine medicine.

These findings notably confirm and expand upon Texty.org.ua's August 2026 publication which explained how "pseudo-medicines" are 'pushed' using Facebook clickbait content, relying on fake news sites. Not only is this a common advertising strategy, our findings raise questions on the implication of the leadership of AdNow in targeting and branding "nutraceutical" content to increase revenue. This is further confirmed by a 2017 job posting, where freelancers were asked to create a "design for a single page landing app with a slider" that was "adapted for the European audience." Attached to the posting is a Google Drive document asking respondents about their weight loss objectives and lifestyles.

## AdNow defunct branch chief recruits freelancers to support United Russia candidate in election cycles

The FL account indicates that the employee would not solely act on behalf of AdNow but also published postings for Yulia Serebryanskaya's non-profit "Russian Initiative ". Using the same email address as listed above, postings recruited freelancers to create the logo of the company and its symbol in 2021.

A 2019 review left by one of the contracted freelancers, also indicated that the account had posted a "personal order" titled "Landing [page] for a parliamentary candidate ".

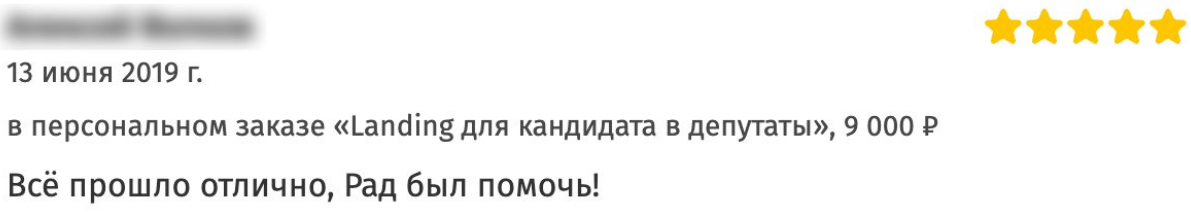


*Figure 15. A screenshot of an FL review from June 13, 2019 about a posting for a "landing [page] for a parliamentary candidate," reading "everything went well. Glad I could help!" (Source: FT[.]ru)*

In 2019, during the Moscow State Duma Elections, Serebryanskaya herself ran for parliament, although she did not win the electoral race. Despite the lack of technical evidence furthering this claim, it remains plausible that AdNow employees recruited freelancers to support Serebryanskaya's campaign online. In addition, Serebryanskaya, has had a long standing relationship with Russia's ruling party United Russia where she reportedly served as the communications director and took part in the presidential campaigns of both presidents Putin and Medvedev.

As reported by Snoop and the Insider, CheckFirst found that the IT infrastructure of companies linked to Serebryanskaya and the former leader of AdNow in Novosibirsk served to host the website of United Russia candidate Alexei Besprozvannykh during the 2024 Governor election in Kaliningrad. Besprozvannykh notably served as deputy Minister of of Industry and Trade of Russia between 2017 and 2024. In 2025, Besprozvannykh was placed under EU sanctions due to his role in "the acquisition of military equipment used in Russia's war of aggression against Ukraine."

CheckFirst identified that the IT company "47Tech," a Serebryanskaya-owned IT firm founded in 2016, registered a domain on IP address 213.171.6[.]223. In 2024, this IP address served to host three domains that supported Besprozvannykh campaign, namely:

- выборы-семья.рф (Elections-Family.rf)
- беспрозванных.рф (Besprozvannykh.rf)
- besprozvannykh[.]ru

| Domain | Type | Property |
|---|---|---|
| xn----9sbco9ajoj9fdp0b.xn--p1ai | IPv4 | 213.171.6.223 |
| xn--80abdlk2badikj0d6d.xn--p1ai | IPv4 | 213.171.6.223 |
| besprozvannyh.ru | IPv4 | 213.171.6.223 |

3 records

Query: ip:"213.171.6.223"

*Figure 16. A DNSLytics screenshot showing three domains historically hosted on IP address 213.171.6[.]223*

That year, these websites were further amplified on Russian social media VK. The page of a Kaliningrad Youth Center notably ran a post calling for action titled "With all the family to the elections!" inviting voters to come with their relatives to the ballots and spread hashtags. The two other domains were used to advertise for Besprozvannykh's campaign and were even linked on the party's official website. In addition, two VK pages invited users to respond to a poll hosted on Besprozvannykh's website.

## Serebryanskaya-linked initiative's IT infrastructure exposes links to European "influencer marketing agencies" and Ad[.]ru

By investigating the IT infrastructure of the "Russian Initiative" CheckFirst established that an IP address hosting the Russian Initiative's website shared links with other Serebryanskaya businesses, including two "influencer marketing" agencies active seemingly since 2022. Our investigation shows deeper links between the Russian Initiative, AdNow, 2WTrade avatars, and connections between Serebryanskaya's businesses.

In 2017, Serebryanskaya founded the non-profit organization "Russian Initiative", which states that its purpose is to safeguard the Russian language and culture, and foster their transmission to next generations. In reality, the organisation also glorifies the USSR and the Russian Empire, claiming to defend of the Russian language to spread pro-Russian patriotic values which its homepage summarizes as "what sets our organization apart is that our primary mission is to unite all Russians living abroad—whether in nearby or distant countries—around a single idea: pride in our great nation."

Hence, the organisation also pursues a global political agenda targeting the perception of Russia and its citizens abroad. Between 2019 and 2021, the Russian Initiative submitted three projects to the Russian Presidential Grant fund, with applications requesting a total of nearly 3.35 million rubles [1] [2] [3]. These projects focused on influencing Russian citizens and Russian language learners abroad stating that "what is taught [abroad] is very different from the Russian idea of our history and culture."

For instance, in 2019, Serebryanskaya and her organisation reportedly advocated for a project focusing on the addition of the Russian word "podvig", meaning "a feat" or "an exploit" to the Oxford dictionary. That year, in an article by Russian press agency IA Realist quoting political technologist Marat Bashirov, a proponent of the initiative, he described it stating that "the question of incorporating the word "podvig" into the international lexicon is highly relevant [..]. In the context of the conflict in the Donbas, for instance, many ordinary people from Russia and other countries traveled there—often under fire—to provide humanitarian aid to those affected. That was a 'podvig'. On the other hand, 'podvig' is a Russian word, and our national idea involves uniting the Russian-speaking population across the globe, as well as those who take an interest in learning the Russian language."

## IP address shares connections with "influencer marketing agencies" and other Serebryanskaya businesses

Between 2025 and 2026, the website of 47Tech, which, as established above, shared an IP address with the Besprozvannykh campaign, was relocated to IP address 185.56.234[.]80. We found that this IP address was also used by Serebryanskaya's Russian Initiative website, as well as other of its businesses such as 2WTrade and Neurostart.

According to the Russian business registry, Serebyranskaya opened the online marketing company Neurostart in 2021. This company, whose Russian sites are now defunct, appears to be linked to two sites registered in 2022, namely tradeuni[.]eu and neurostart[.]eu. The Neurostart website notably states that "Neurostart is a platform for bloggers. Work with a Instagram, TikTok, YouTube and Facebook blogger marketplace. Join us to become a celebrity. " It also features versions in English ("British" on the websites), Russian, French, Italian, German and Swedish. While Neurostart is registered, UniTrsade does not appear as a Serebryanskaya registered business although the website structure and IP hosting point towards a shared owner.

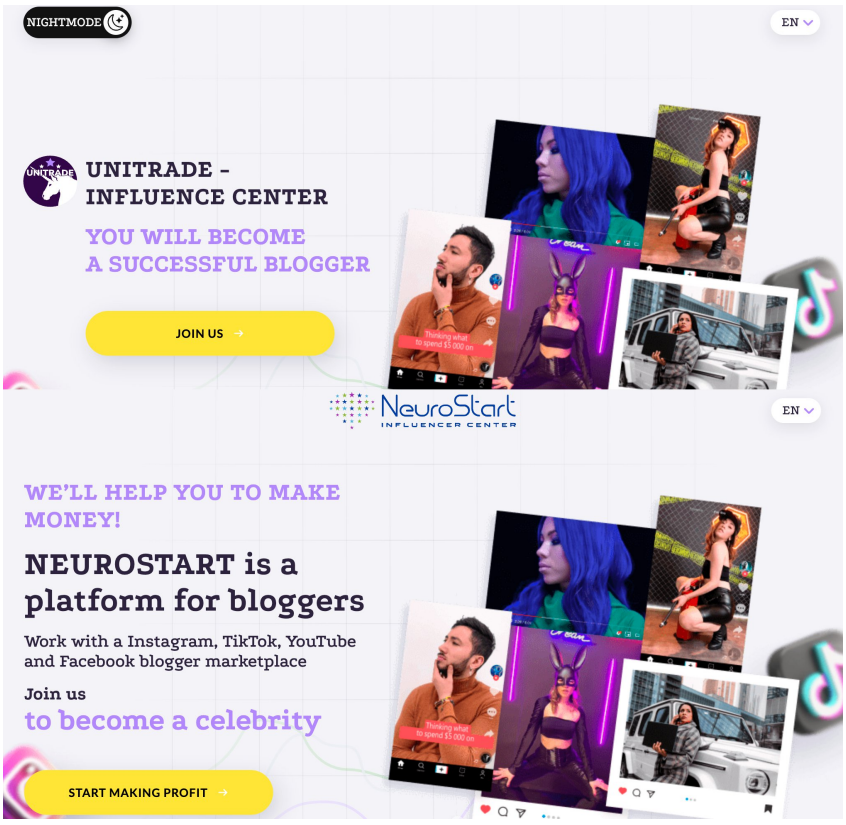


*Figure 17. Screen captures of supposed "influencer agencies" websites unitrade[.]eu and neurostart[.]eu. (Sources: tradeuni[.]eu/archive, neurostart[.]eu/archive)*

The webpages of these sites also feature logos of alleged brands witch which the "influencer agencies" have collaborated, including Viteddy, as well as Latte Beauty for which AdNow staff member placed jobs to recruit three freelancers on FL [1] [2] [3].

The oldest records of the domains hosted on this IP address further indicate that it was used by the Russian advertising and gambling forum AdDays since 2017. The Russian Initiative's domains youfri[.]ru, youfrom[.]ru as well as Serebryanskaya's personal site, serebryanskaya[.]ru have also been hosted on this IP address between 2018 and 2023.

According to DNSLytics data, the only other active co-hosted site on IP address 185.56.234[.]80 is tophot[.]com whose purpose remains unknown. However, WHOIS records indicate that ownership of the website belongs to the company Asset Management, which reportedly also belongs to Serebryanskaya according to business register data. In addition, the registration address in Moscow's Varshavskoye Shosse is similar to AdNow's former location. The email address referenced in the WHOIS record also seems to belong to Yulia Serebryanskaya, as further WHOIS records indicate that this email address served for the registration of domains 47element[.]com (linked to 47Tech), and lattebeauty[.]com — which appears along Viteddy as the brands sponsoring Neutrostart —.

```
Domain Name: TOPHOT.COM
Registry Domain ID: 96684416_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.nic.ru
Registrar URL: https://www.nic.ru
Creation Date: 2003-04-10T18:10:42Z
Registrar Registration Expiration Date: 2027-01-01T21:00:00Z
Registrar: Regional Network Information Center, JSC dba RU-CENTER
Registrar IANA ID: 463
Registrar Abuse Contact Email: tld-abuse@nic.ru
Registrar Abuse Contact Phone: +74959944601
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: OBShchESTVO S OGRANIChENNOY OTVETSTVENNOSTU ESSET MENEDZhMENT
Registrant Organization: OBShchESTVO S OGRANIChENNOY OTVETSTVENNOSTU ESSET MENEDZhMENT
Registrant Street: Varshavskoe d 1 str 1 kom 38
Registrant City: g Moskva
Registrant State/Province: g Moskva
Registrant Postal Code: 117105
Registrant Country: RU
Registrant Phone: +7.9232515356
Registrant Phone Ext:
Registrant Email:
```

*Figure 18. A screencapture of WHOIS records for website tophot[.]com (Source: DNSLytics).*

## AdRu, AdNow and Fazze?

Finally, historical data locating the premises of AdNow in Novosibirsk shows that the company's location may have been used by other companies over time. Its Novosibirsk address notably also served for the now-defunct company AdRu, whose domain adru[.]pro remained active until 2024. Its reported phone number was also used by AdNow. In one case even AdNow's page on a local Novosibirsk website linked to the adru[.]pro domain.

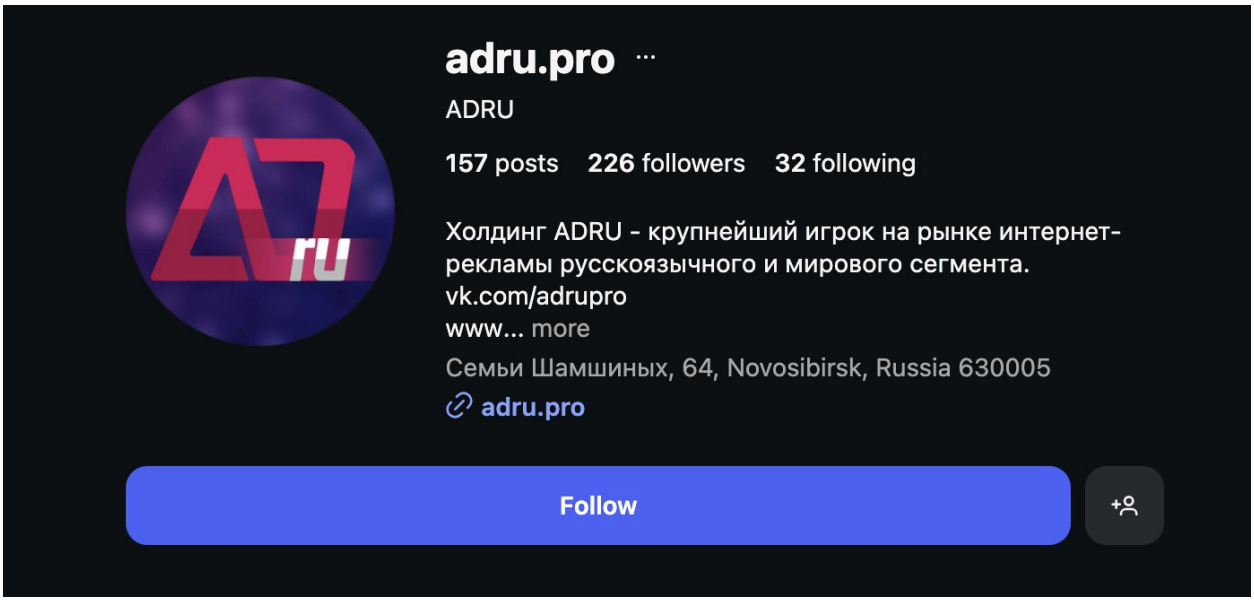


*Figure 19. Screenshot of adru.pro's Instagram page. (Source: Instagram)*

This is also confirmed by business register data showing that the same entity shared its address with AdNow. Further, according to historical IP address 5.187.7[.]36 record data, AdNow's servers shared the same IP address as as the domains "ads1-ad[.]ru" and subdomains of the domain "adonweb[.]ru ". The latter was notably used as a username by Novosibirsk employee whose email was contained in recorded auction data.

Further, as exposed above, Serebryanskaya domains frequently shared IP resources with the Russian Initiative and 47Tech. According to DNSLytics data, the IP address 88.208.35[.]225 which hosted Serebryanskaya's 2WTrade and the Russian Initiative's wesbites, also hosted the domain ad[.]ru between 2018 and 2019 as well as between 2021 and 2024.

According to additional historical data for IP address 88.208.58[.]194 on which fazze[.]com was located, we also found that the domain ad[.]ru was located on this IP address until 2015.

Although this does not constitute irrefutable proof of the coordination between Serebryanskaya's entities, AdNow and Fazze, this constitutes infrastructural overlap that should draw researchers' attention.

## Conclusion

Over the course of this investigation, it has become clear that advertising companies play a key role in providing revenue to deceitful online actors and reward the dark patterns they exploit to generate more gain. Our findings only scratch the tip of an iceberg of inauthentic online assets, whose only aim is to entice users and exploit online communities to increase profits and drive engagement. While not entirely illegal, these practices also question the responsibility of the advertising companies enabling such behaviour and ultimately, cashing in on these enterprises too.

Our research further indicates that the lines between opportunity sellers and buyers in the case of AdNow may be more blurrier than previously imagined. By engaging in placing adverts from offer domains that reportedly engage in phishing, scam and the placement of health supplements presented as genuine medicine, the company definitely plays a role in the enterprises described above. Furthermore, our investigation shows that the reported staff and leadership associated with AdNow, has been taking part in the designing of deceitful online products, particularly nutraceutical and landing pages, by hiring freelancers.

Also, our research raises questions regarding AdNow's role and the implications of doing business with a company that has on occasions supported and provided IT infrastructure to a candidate from Russia's ruling party under EU sanctions and shares links to presidents Medvedev and Putin. In the wake of the 2022 invasion of Ukraine by Russia, the predatory logic at play in the deceitful online campaigns we exposed and the revenue generated by a company that remains in close proximity with the Russian power raises ethical and legal concerns. Despite IAB Europe's reported restriction imposed against AdNow to "place advertising through its centralized real-time bidding system," and Romania's ANCOM public warnings regarding online assets and Facebook pages linked to the company, AdNow's activity remains at large, with a target that is only widening and most certainly encompasses more countries than those we were fortunate enough to identify.

# Appendices

## Appendix 1. AdNow domains.

| Domain |
|---|
| adnow[.]com |
| ads1-adnow[.]com |
| ads3-adnow[.]com |
| ads7-adnow[.]com |
| n.ads7-adnow[.]com |
| gorgind[.]com |

## Appendix 2. AdNow's n.nnowa[.]com reverse engineered endpoints.

| Path | Method | Purpose |
|---|---|---|
| /a | GET (Script) | Ad request - returns JavaScript with ad configuration |
| /st | GET (Pixel) | Impression tracking (full block) |
| /stn | GET (Pixel) | Individual teaser impression tracking |
| /stv | GET (Pixel) | Viewability tracking (full block) |
| /stnv | GET (Pixel) | Individual teaser viewability tracking |
| /click | GET | Click tracking (on gorgind.com) |

## Appendix 3. Captures per domain.

| Domain | Network | Captures |
|---|---|---|
| adskeeper[.]com | AdsKeeper | 5,068 |
| adnow[.]com | AdNow | 7,398 |
| c.mgid[.]com | MGID | 5,141 |
| n.nnowa[.]com | AdNow | 4,023 |
| ads1-adnow[.]com | AdNow | 636 |
| ads7-adnow[.]com | AdNow | 1,908 |
| mgid[.]com | MGID | 5,273 |
| c.adskeeper[.]com | AdsKeeper | 16,484 |

## Appendix 4. RomaniiNostri[.]ro linked Facebook assets.

| Name | URL |
|---|---|
| La mine acasa in Romania. | https://www.facebook[.]com/lamineacasainromania |
| Mesaje frumoase | https://www.facebook[.]com/profile.php?id=100068240211055 |

| | |
|---|---|
| de "La multi ani" | |
| Puterea Iubirii | https://www.facebook[.]com/PuterealubiriiReala |
| Glume interesantee | https://www.facebook[.]com/glumepentruvoi |
| Suflet Călător | https://www.facebook[.]com/profile.php?id=61555844099582 |
| 2antisociali | https://www.facebook[.]com/profile.php?id=61556278405416 |
| Umor Bun | https://www.facebook[.]com/umorbun |
| Ziua Bună | https://www.facebook[.]com/rugaciuneainimii1 |
| Tezaur de Curiozități | https://www.facebook[.]com/profile.php?id=61558989205458 |
| Muzică și Citate | https://www.facebook[.]com/elena.tudor44 |
| Mesaje Frumoase | https://www.facebook[.]com/peisaje70 |
| Inima de mama | https://www.facebook[.]com/profile.php?id=100068771946706 |
| MOOD | https://www.facebook[.]com/moodblogromania |

## Appendix 5. ExtraNews[.]ro linked Facebook assets.

| Name | URL |
|---|---|
| Amintiri frumoase | https://www.facebook[.]com/1.RO.1Amintiri |
| I Love You. | https://www.facebook[.]com/iloveyou.teiubesc |
| DRAGOSTEA MEA | https://www.facebook[.]com/dragosteameaaaa |
| Parintele Calistrat | https://www.facebook[.]com/profile.php?id=100077906862412 |
| Iubire & Trădare | https://www.facebook[.]com/Ela.Mitachi |
| Regretele Unei Femei | https://www.facebook[.]com/Stefania.AndreeeaaaOfficialPage |
| Cinematografia Veche | https://www.facebook[.]com/cinematografiavecheofficial |
| Natura cu frumusetile ei | https://www.facebook[.]com/naturacufrumusetile |
| Un suflet | https://www.facebook[.]com/Un.Suflet |

## Appendix 6. hraparaknews[.]am linked domains.

| Domain | IP address |
|---|---|
| harcum[.]am | 95.142.40[.]92 |
| dushrasskazi[.]ru | 95.142.40[.]92 |
| arminfonews[.]ru | 95.142.40[.]92 |
| joxovurdnews[.]am | 95.142.40[.]92 |
| mybook[.]am | 95.142.40[.]92 |
| erevanblog[.]am | 95.142.40[.]92 |
| hraparaknews[.]am | 95.142.40[.]92 |
| usmedtrade[.]com | 95.142.40[.]92 |
| iispania[.]com | 95.142.40[.]92 |

| | |
|---|---|
| newslur[.]am | 95.142.40[.]92 |
| orertert[.]am | 95.142.40[.]92 |
| ikekioik[.]online | 95.142.40[.]92 |
| hayreniq[.]am | 95.142.40[.]92 |
| ikekujoik.online | 95.142.40[.]92 |
| eastvillageleslieville[.]com | 95.142.40[.]92 |
| korrespondent[.]am | 95.142.40[.]92 |
| kommersant[.]am | 95.142.40[.]92 |
| ameolik.online | 95.142.40[.]92 |
| bbcnews[.]am | 95.142.40[.]92 |
| amerikok.online | 95.142.40[.]92 |
| fransi.online | 95.142.40[.]92 |
| smekiik.online | 95.142.40[.]92 |
| leaderland[.]am | 95.142.40[.]92 |
| ukrainaok[.]ru | 95.142.40[.]92 |
| gazeta[.]am | 95.142.40[.]92 |
| 168news[.]am | 95.142.40[.]92 |
| araratlur[.]am | 95.142.40[.]92 |

## Appendix 7. bestzone24.biz[.]ua linked domains

| Domain | MGID tag |
|---|---|
| bestzone24.biz[.]ua | N/A |
| dailystar.biz[.]ua | MGID-939000 |
| every24.com[.]ua | MGID-939000 |
| timer.biz[.]ua | MGID-939000 |
| zoneinfo24.biz[.]ua | MGID-939000 |
| zwierzeta.biz[.]ua | MGID-939000 |
| fakt24.biz[.]ua | MGID-939000 |
| strefa24.biz[.]ua | MGID-939000 |
| planetta.biz[.]ua | MGID-939000 |
| infos24.biz[.]ua | MGID-728167 |
| everyday.pl[.]ua | MGID-728167 |
| ciekawe24.pl[.]ua | MGID-728167 |
| mytimes24.biz[.]ua | MGID-728167 |
| day24[.]info | MGID-728167 |
| swiat24.pl[.]ua | MGID-728167 |
| faktow.biz[.]ua | MGID-728167 |
| narrod.biz[.]ua | MGID-728167 |
| dailytimes.biz[.]ua | MGID-728167 |
| derzhava365.biz[.]ua | MGID-728167 |
| fakty24.pl[.]ua | MGID-728167 |
| mytime24[.]info | MGID-728167 |

| | |
|---|---|
| interesting24[.]com | MGID-728167 |
| info21[.]pro | MGID-728167 |
| timezones24.biz[.]ua | MGID-728167 |
| story24.biz[.]ua | MGID-943625 |
| livecity.biz[.]ua | MGID-943625 |
| aktualnosci.pl[.]ua | MGID-943625 |
| lifevery.biz[.]ua | MGID-943625 |
| lifestory.biz[.]ua | MGID-943625 |
| ciekawi.pl[.]ua | MGID-943625 |
| daylife.pl[.]ua | MGID-943625 |

## Appendix 8. vendeto[.]am linked inauthentic Facebook pages

| Name | URL |
|---|---|
| Já a moje Česká republika | https://www.facebook[.]com/profile.php?id=61577845354894 |
| Šťastná Česká republika | https://www.facebook[.]com/profile.php?id=61579559591548 |
| Az én gyönyörű Magyarországom | https://www.facebook[.]com/profile.php?id=61576788763096 |
| Já a moje krásná Česká republika | https://www.facebook[.]com/profile.php?id=61576833390301 |
| Moje rodina | https://www.facebook[.]com/profile.php?id=61576488988888 |
| Historia De Emoción | https://www.facebook[.]com/profile.php?id=61576432213321 |
| Já a Česká republika | https://www.facebook[.]com/profile.php?id=61576588796157 |
| Já a moje Česká republika | https://www.facebook[.]com/profile.php?id=615800260401 53 |
| Já a moje Česká republika | https://www.facebook[.]com/profile.php?id=61576481591271 |
| Zajímavé příběhy v Česku | https://www.facebook[.]com/profile.php?id=61577258527330 |

## Appendix 9. Domains using gns.gdnst[.]pro as name server.

| Domain | NS |
|---|---|
| ads1-adnow[.]com | gns.gdnst.pro |
| ads5-adnow[.]com | gns.gdnst.pro |
| nnowa[.]com | gns.gdnst.pro |
| ads7-adnow[.]com | gns.gdnst.pro |
| ads6-adnow[.]com | gns.gdnst.pro |

| | |
|---|---|
| certdmn[.]com | gns.gdnst.pro |
| gacloop[.]info | gns.gdnst.pro |
| mgacloop[.]info | gns.gdnst.pro |
| lofkut[.]com | gns.gdnst.pro |
| gdnst.pro | gns.gdnst.pro |
| lacloop[.]info | gns.gdnst.pro |
| mlacloop[.]info | gns.gdnst.pro |
| horkwist[.]com | gns.gdnst.pro |
| jolkt[.]com | gns.gdnst.pro |
| forfdfp[.]com | gns.gdnst.pro |
| klodrum[.]com | gns.gdnst.pro |
| click116[.]com | gns.gdnst.pro |
| yamsty[.]com | gns.gdnst.pro |
| 116wgt.online | gns.gdnst.pro |
| gorgind[.]com | gns.gdnst.pro |
| lologh[.]com | gns.gdnst.pro |
| bfxssp[.]com | gns.gdnst.pro |
| mgacloopb[.]info | gns.gdnst.pro |
| 116clk[.]online | gns.gdnst.pro |