NISOS TRADECRAFT

Tracking Down Potential Disinformation Domains and Marketplaces

June 2023

RESEARCH

NISOS

Nisos Tradecraft: Tracking Down Potential Disinformation Domains and Marketplaces

A Domain Analysis: Russian Sleight-of-Hand or Legit Change of Ownership?

25 May 2023

Threat intelligence involves a lot more than just looking at a stream of logs, a firehose of API data, or a mountain of malware. It requires digging through various current and historical data sources to identify individuals or entities involved in threat activity. By examining a threat actor's behavior, you can prepare a detection plan that moves beyond the limitations of traditional incident response. Sometimes, investigating a potential threat indicator is a gold mine of data, other times, not so much.

Some of our clients are interested in abiding by sanctions laws, and avoiding organizations that may use their corporate platforms or other resources to bypass sanctions or get an incendiary political message across. Occasionally, domains involved in such endeavors change ownership data in WHOIS records to make it look like the owner of the domain has changed in an attempt to maintain control of the infrastructure when they suspect it has been exposed.

Russian disinformation networks notoriously love wading into US politics, and when there's rubles involved, opportunism can trump ideology. In this case, Nisos identified a once-pro Kremlin domain—putinlive.com—used by the Russian social media and marketing company IMA Consulting that is now registered to "Against Trump Media." IMA Consulting is one of Russia's largest marketing firms and is known for creating websites that serve Kremlin interests, including campaign sites for Russian President Vladimir Putin's 2018 presidential campaign and the referendums for occupied Ukraine to vote to join Russia. Official procurement records show that the Russian government has awarded billions of rubles worth of contracts to IMA Consulting's parent company, IMA Group, and its 10 subsidiaries.

- The domain putinlive.com was registered to IMA Consulting in April 2017, according to domain registration data.[1] In March 2022, control of the domain appeared to change.
- On 14 March 2022, GoDaddy appeared as the registrar with no owning organization listed. Approximately one week later, Against Trump Media took control of the domain. The domain registration information listed a Delaware address, phone number, and an email: usvs45@gmail.com.

[1] Domain registration data shows the domain was re-registered to a private individual in August 2017 and was registered by a Russia-based registrar through 2022. Nisos did not investigate these intermediate owners as part of this study.

Throughout the course of the investigation, answers often lead us to more questions and inform the path the investigation takes. At every twist and turn we dig deeper for the full story.

Faced with the above data, we are left to ask ourselves the following questions:

Does the switch from a Russian owner to a Delaware-based entity represent a legitimate ownership change or simply a way to hide true ownership?

Given Russian interference in previous US elections, Nisos researched the site's content for evidence that it propagated political influence or disinformation and investigated the people behind Against Trump Media to determine whether Russian-government linked entities still controlled the domain.

Is the site engaged in political influence?

On 15 May 2023, putinlive.com redirected to another politically-oriented website titled trumpisscrewed.com. The site contained an image with an anti-Trump bias (shown below), but it did not look like a traditional political influence or disinformation site. The site did not feature articles, memes, or other content. Additionally, the site listed over 150 separate sites—almost all of which had titles relating to political candidates or Russia and Ukraine—under a section "domains for sale."

Graphic 1: Trumpisscrewed.com header

When Nisos first researched this domain in February 2023, the url redirected to a different site with similar content: https://kevinmccarthyagainsttrump.com/. The kevinmcarthy site also contained a section discussing the importance of livestreaming for disseminating political messaging.

The “contact us” section contained a Phoenix, Arizona phone number and an image containing the words fucktruth.social. These selectors will later lead us to the man behind Against Trump Media.

Now that we have collected and identified all the relevant details, we need to synthesize what we have into something actionable to our clients and decide whether we have enough information, or whether we need to dig even deeper!

What is Against Trump Media?

A general open source search for the organization Against Trump Media yielded several social media accounts and a webpage, againsttrumpmedia.com. All of these pages are very obviously anti-Trump and link to numerous other sites with domain names that advertise their stance on former President Trump. Examples include vetsagainsttrump.com, pastorsagainsttrump.com, and stoptrump.today.

AgainstTrumpMedia.com also now redirects to trumpisscrewed.com, but archived versions of the site from January 2018 claim it was originally set up to support a political movement against Trump. Its website states, “Against Trump Media is a digital ecosystem...powered with influencer marketing and fueled by user generated content…Our network of websites and supporting social media platforms is the engine under the ‘hood’.”

By August 2018, the site had shifted from disseminating or encouraging anti-Trump content to simply offering a list of 125 “premium anti-Trump” domains for sale. This was a clue that Against Trump Media might be a profit-motivated venture.

Who is behind Against Trump Media?

Against Trump Media LLC, company number 6667852, was registered in December 2017 in Delaware, which does not require owners, members, or managers to be listed on the company formation documents. Nisos then examined all the selectors identified previously in our research to attribute the people behind the company.

Selectors connected to the domain ultimately show a businessman, Rex Powers, as the founder and organizer of Against Trump Media.

- A single archived version of againsttrumpmedia.com listed a Linkedin account for Rex Powers. The email on the putinlive domain registration, USvs45@gmail.com, had the partial email rex*******@gmail.com as its recovery email, almost certainly a reference to the same Rex Powers.
- The Against Trump Facebook page contains an email on the domain antitrumpdomains.com, which in 2017 was registered to a Rex Powers with an organization name of RexPowers.com.
- The Twitter account @USvs45 as of 15 May 2023 now uses the display name TuckerCarlson.live, but archived versions of this account show it previously used the displayname

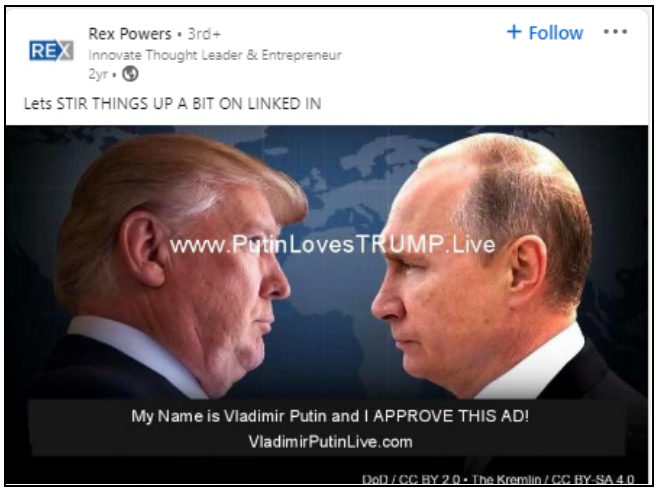
FuckTruth.social, which matches the image and display name from the “Contact Us'' section of trumpisscrewed.com. A review of the @USvs45’s post showed that it linked to Rex Powers’s LinkedIn account in March 2022.

Graphic 2: Link to Rex Powers’s LinkedIn from USvs45’s Twitter account.

So what’s with all these domains?

Nisos concluded that Powers most likely leveraged these domains to promote votes against Trump prior to the 2020 election, but ownership of these domains now is largely profit motivated.

- Against Trump Media announced it would sell its digital assets using the Grrr8Domains division of Powers Family Holdings (PFH) in a 2019 press release. PFH’s domains-for-profit business is more extensive than just the domains used for Against Trump Media; PFH had been involved in the sale of political-themed domains since 2016 and its subsidiary Grrr8Domains has domains related to cannabis, job hunting, live streaming, real estate, and product reviews up for sale.
- A review of Powers’s LinkedIn posts shows that he posted anti-Trump content on these domains. Posts from two to three years ago include anti-Trump messaging with mentions of the domain name. More recently, his posts advertise the value of his domains for use in political marketing or influence. As examples, earlier this year, he wrote an article about the risk of strategic redirects and domain name squatting as well as a post about the value of .live domains for use by streamers.



Graphics 3 and 4: Two posts from Rex Powers's LinkedIn account disparaging former President Trump posted two and three years ago.

Graphic 5: Recent post from Powers's LinkedIn account illustrates the switch to promotional from political posts.

Conclusion

Nisos ultimately found no connection between Powers or Against Trump Media with any Russian marketing agencies. However, to reach this conclusion, Nisos had to leverage WHOIS data, corporate registration data, analysis of social media, and traditional open source searches to attribute the company and person behind a website.

In this case, then, the switch of domain ownership from a Russian marketing firm to a Delaware-based entity represented a legitimate ownership change. Sometimes it's not Putin…sometimes it's just a guy trying to make some money.

Regardless of the outcome, our client investigations culminate in an intelligence briefing. When real threats are identified, we provide all the context and an executive summary with specific recommendations about how to mitigate the client's risk, shut down the threat, and/or prevent it from happening in the future. When the intelligence concludes that there is no threat, this too is actionable intelligence. The client knows with confidence that this is not a risk that warrants further action nor loss of sleep.

About Nisos®

Nisos is The Managed Intelligence Company®. Our analyst-led intel investigations, assessments, and monitoring services empower your security, intelligence and trust and safety teams. We provide accurate, customized intelligence that guides your security and risk decisions – protecting your organization, assets, and people. Learn more at nisos.com.