Writing with Invisible Ink

By the Alethea Team

ALETHEA

alethea.com

EXECUTIVE SUMMARY

In February and March 2024, Alethea uncovered 5,314 accounts on X (formerly known as Twitter) and 81 websites that we assess are likely being leveraged to further operations of the main Russian military intelligence directorate, commonly known as the GRU.

Based on the content and behaviors of these assets, we believe this network is a continuation of a persistent Russian influence operation known as Doppelgänger, which was initially exposed in 2022 but to date had not been attributed to a specific governmental entity, though recent reporting, based on leaked documents, has indicated a link to the office of the Russian President. The network seeks to influence citizens in the U.S., Germany, France, and other nations supportive of Ukraine to erode political, financial, and military support for its war effort.

The network demonstrates a shift in Russian objectives as it relates to the elections. To date, in the United States, Russian influence operations have amplified opposing perspectives on both sides of the political spectrum and exploited a range of politically sensitive issues. Now, the objective is to support candidates and amplify issues that reduce support for Ukraine. Russia is spreading multiple messages to amplify narratives in the United States that create false dichotomies on domestic issues like border security, inflation, unemployment, and general criticism of the Biden Administration. In lieu of amplifying narratives on both sides, the narratives Alethea observed will inevitably benefit conservative candidates; however, Alethea has no evidence to suggest that candidates or parties benefiting from these efforts are wittingly participating.

The network also signals a maturation of Russian tactics to attempt to avoid detection, though nothing can guarantee going undetected. This network is using a new tactic, which Alethea dubs “Invisible Ink,” an amplification tactic. For researchers or security professionals to obtain data via the X (formerly known as Twitter) API, they rely upon searches that use specific keywords or known accounts. The network Alethea assessed appears to be evading detection by researchers, security firms, and its targets by copying and pasting specific tweet URLs in lieu of retweeting or posting, requiring threat intelligence teams to know the exact tweet URL in order to find amplification accounts, which are assigned when the original tweet is created. In other words, to detect the accounts amplifying this content would require the list of unique tweet URLs to obtain the data.

Alethea assesses this network is only a fraction of the overall operation, and anticipates that accounts will be continuously created and deployed to advance Russian military interests. At the time of writing, US elections are several months away and Alethea anticipates that the Russians will continue to deploy, test, and iterate on their efforts.

Alethea conducted this investigation to alert voters, candidates, and governments alike to these novel tactics employed by affiliates of the Russian state. As elections approach in the U.S. and dozens of other countries worldwide, continually exposing the evolving features of Russian influence operations will help mitigate their effects on democratic discourse. If we all have eyes on the adversary, and work to expose their tactics, our collective defense can safeguard democracies worldwide.

KEY TAKEAWAYS

Alethea assesses that this network is likely affiliated with or otherwise working to promote GRU owned content.

The network is almost certainly affiliated with the Russian influence operation Doppelgänger based on an analysis of X (formerly known as Twitter) accounts. Our investigation uncovered a series of likely connections to Russia's main military intelligence service, commonly known as the GRU, and thus Alethea assesses that Doppelgänger is likely being leveraged to further GRU operations.

Alethea observed that this network is being leveraged by GRU entities. It makes this assessment based on overlap in sanctions of GRU-linked outlets alongside Russian companies, Structura and Social Design Agency, with pro-Kremlin ties, in addition to other indicators. Specifically, Structura is a subsidiary of Rostec, the main Russian defense contractor.

Accounts in this network shared links to Observateur Continental and EuroBRICs, both associated with InfoRos, which was sanctioned by the U.S. Treasury Department in 2021 due to its affiliation with GRU Unit 54777, otherwise known as the 72nd Special Service Center.

Invisible Ink, a term dubbed by Alethea, describes a novel content amplification technique on X during the course of this investigation.

We named it Invisible Ink because the posts are only likely to be found by investigators who know precisely which tweets to look for, as if they are written with invisible ink.

The technique involves quote posting other assets' content with no additional text, using standard X platform features to inauthentically amplify content and extend their reach and potential impact on target X users.

Since the posts do not contain any text, it is nearly impossible to find these posts without already knowing their specific URLs or the account's username.

Specifically, these quote posts are shared in ongoing conversation threads. This means that the unsuspecting users to whom they reply receive a notification from these "bot" accounts, which contains the Doppelgänger content.

Accounts in this network had one of two distinct functions: one group of accounts published the Doppelgänger content, while the other used Invisible Ink to spread this content among legitimate X users outside of the network.

The Kremlin appears to have shifted its strategy from sowing division in target democracies to a sole focus on undermining support for Ukraine in democracies.

We assess that narratives may shift as the operation observes what resonates and based on world events, and we anticipate that the effort will continue to focus on protectionist, isolationist, and other narratives in order for Russia to achieve a weaker Ukraine with fewer resources. Currently, that means that Russian operatives are likely supporting conservative candidates, although Alethea has no evidence to suggest that the candidates are aware of this prior to writing this report.

Russia uses Invisible Ink assets to promote positions and candidates in the United States, Germany, and France generally opposed to continued military aid to Ukraine and occasionally Israel, usually found among right-wing audiences, on X.

The posts we collected from this network were often published in the first person, creating the appearance of a local citizen's personal opinion, and tended to promote conservative views of enhanced border control and isolationist narratives while denigrating the current U.S. administration. Posts often suggested that military aid to Ukraine or, at times, Israel, should be diverted to domestic security and economic issues.

Previous Russian information operations manipulated discourse across the political spectrum, but we observed that assets using Invisible Ink almost exclusively target conservative voters. Prior to the release of this report, Alethea does not have evidence to suggest that conservative parties are aware of this network and its amplification of conservative viewpoints or degradation of the current Administration.

The operation continues to make use of cloned websites for global news outlets, as well as creating their own sites with original content.

The sites cloned by the operation show some of the important geographic targets for the Russians, including cloning Fox News, The Guardian, Le Monde, and Spiegel.

If a user clicks on a link shared by accounts in this network, they will unknowingly be automatically redirected three times though other intermediary websites before seeing the clone website. This distances the final destination URL from post on X, potentially lowering the risk that the URL will be restricted or blocked from the platform.

In addition to the links shared to sanctioned entities described above, Alethea also observed an instance of this network linking to a website affiliated with the Natural News family of websites, which has been accused of spreading disinformation.

Based on analysis of their IP addresses, we assessed that many of the domains shared by this network were controlled by Russian entities.

INTRODUCTION

In February 2024, Alethea investigated an initial batch of 2,129 X accounts, which we assessed are part of the Doppelgänger network, based on the use of the same tactics, techniques, and procedures (TTPs) previously reported in other external investigations.

In the course of the analysis, we uncovered an additional 3,185 accounts that we assess with high confidence to be part of the same overall network. This network targets conservative segments of the U.S., German, and French electorates ahead of their 2024 elections, amplifying discontent with foreign aid spending to erode support for Ukraine. In our investigation, we observed a significant shift in Russia's influence operations strategy, particularly as it relates to global elections, that threatens the integrity of election discourse.

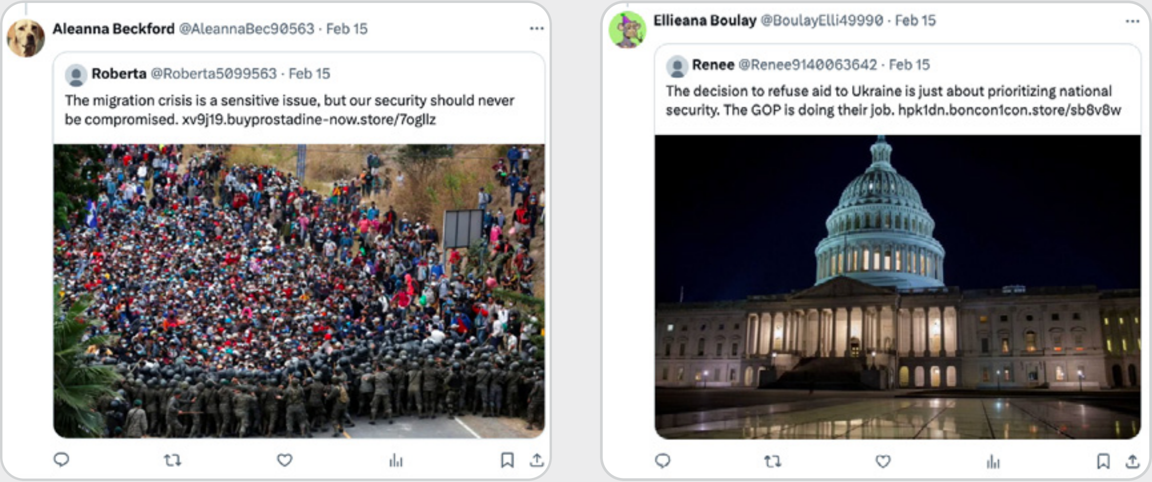
Alethea has consistently tracked efforts by a variety of actors, including state actors, to influence the United States' elections using covert influence operations since 2019. In previous elections, Russian information operations manipulated discourse across the political spectrum by exploiting politically sensitive issues in US and other NATO ally countries. In 2024, their campaigns have one clear objective: winning the war Russia waged against Ukraine. To this end, Russia uses Doppelgänger assets to promote right wing positions and candidates, who are generally opposed to continued military aid to Ukraine.

Based on the findings of our investigation, Alethea concluded that this network is leveraged by the GRU. Of the 81 domains shared by accounts in our analysis, the vast majority of which were either cloned versions of international news sites or originally created outlets, two had overt ties to the GRU. Assets in this network shared links to Observateur Continental and EuroBRICs, known assets of Russian state media network InfoRos, which were sanctioned by the

U.S. Department of the Treasury due to their affiliation with GRU Unit 54777, otherwise known as the 72nd Special Service Center.[1] [2] Notably, we did not observe content from sources attributed to other Russian intelligence services being shared.

In the United States, narratives disseminated by the Russian network include the following:

- Calls to cease **funding for Ukraine or Israel suggested these resources should instead be diverted to domestic issues**, such as domestic border security
- The posts in our analysis tended to promote conservative views of enhanced border efforts and isolationist narratives while denigrating the current US administration. Given the apparent affiliation with the Russian military, **this is consistent with Russia's broader military interests**



Aleanna Beckford @AleannaBec90563 · Feb 15

Roberta @Roberta5099563 · Feb 15

The migration crisis is a sensitive issue, but our security should never be compromised. xv9j19.buyprostadine-now.store/7ogllz

Ellieana Boulay @BoulayElli49990 · Feb 15

Renee @Renee9140063642 · Feb 15

The decision to refuse aid to Ukraine is just about prioritizing national security. The GOP is doing their job. hpk1dn.boncon1con.store/sb8v8w

Invisible Ink assets remarked on the U.S. border crisis and aid to Ukraine using the first person to suggest they are Americans.[3] [4]

[1] https://home.treasury[.]gov/news/press-releases/jy0126

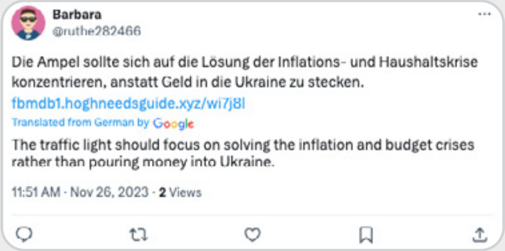
[2] https://www.disinfo[.]eu/publications/how-two-information-portals-hide-their-ties-to-the-russian-news-agency-inforos/

[3] https://x[.]com/AleannaBec90563/status/1758294637830094939

[4] https://x[.]com/BoulayElli49990/status/1758209978098229596

- We observed a new behavior where Doppelgänger accounts linked to third-party content instead of their original content on cloned websites. Specifically, we saw them **link to a website associated with the Natural News network**; this was most likely a target of opportunity based on similar and friendly narratives, and **Alethea does not have evidence to suggest that Natural News is affiliated with or witting to the operation**.
- We observed a small portion of **accounts posing as cryptocurrency promoters**, potentially as a method of avoiding detection for coordinated inauthentic behavior or to appeal to crypto users.

Russian efforts included other countries as well, including Germany, Israel, and other NATO countries. Among the posts we collected, these narratives include:



Barbara
@ruthe282466

Die Ampel sollte sich auf die Lösung der Inflations- und Haushaltskrise konzentrieren, anstatt Geld in die Ukraine zu stecken.
fbmdb1.hoghneedsguide.xyz/wi7j8l

Translated from German by Google

The traffic light should focus on solving the inflation and budget crises rather than pouring money into Ukraine.

11:51 AM · Nov 26, 2023 · 2 Views

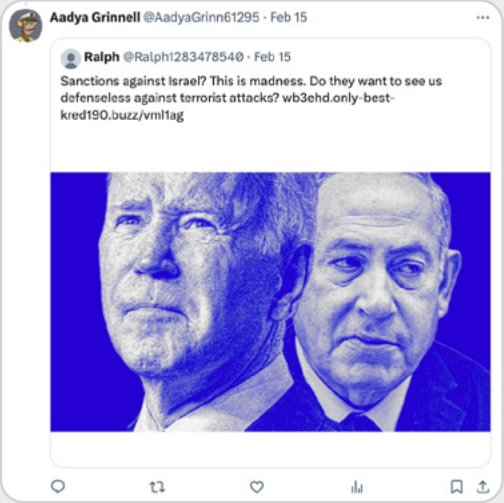
A German-language post suggests that the Traffic Light Coalition should stop funding Ukraine and instead focus on domestic economic issues.

https://x[.]com/ruthe282466/status/1728818833929166905

- English-, German-, and French-language political posts centered on protectionist, anti-war themes that will likely be key **considerations for the 2024 elections**. These accounts amplified the farmer protests in German.
- Other accounts similarly posed as Japanese-language users, publishing a **mix of Invisible Ink posts and unrelated reposts in Japanese**. For example, these accounts posted approximately 4 original posts in Japanese and 100 reply posts amplifying Ukrainian-language videos.

The network itself shows an increased sophistication by the GRU. Accounts using personas to resemble voters posted original content in the first person, creating the appearance of a local citizen's personal opinion. The accounts were then amplified using a new tactic Alethea uncovered, that we call **Invisible Ink**. **This technique involves using X's quote-posting function to share other assets' content** with no additional text, inauthentically amplifying content while attempting to evade detection by both moderators and researchers.

We suspect that there are almost certainly thousands more accounts leveraging these techniques that are likely a part of this operation, and we observed that accounts continue to be created by the same or similar actors. By exposing this technique and clearly connecting it to the Russian state, we hope to help audiences better understand how U.S. adversaries use social media as a tool of information warfare, and support the broader field in stopping the adversary.



Aadya Grinnell @AadyaGrinn61295 · Feb 15

Ralph @Ralph1283478540 · Feb 15

Sanctions against Israel? This is madness. Do they want to see us defenseless against terrorist attacks? wb3ehd.only-best-kred190.buzz/vml1ag

An English-language post in the first person, as if to suggest the user is Israeli, disparaged sanctions placed on four Israeli citizens by the United States in early February.

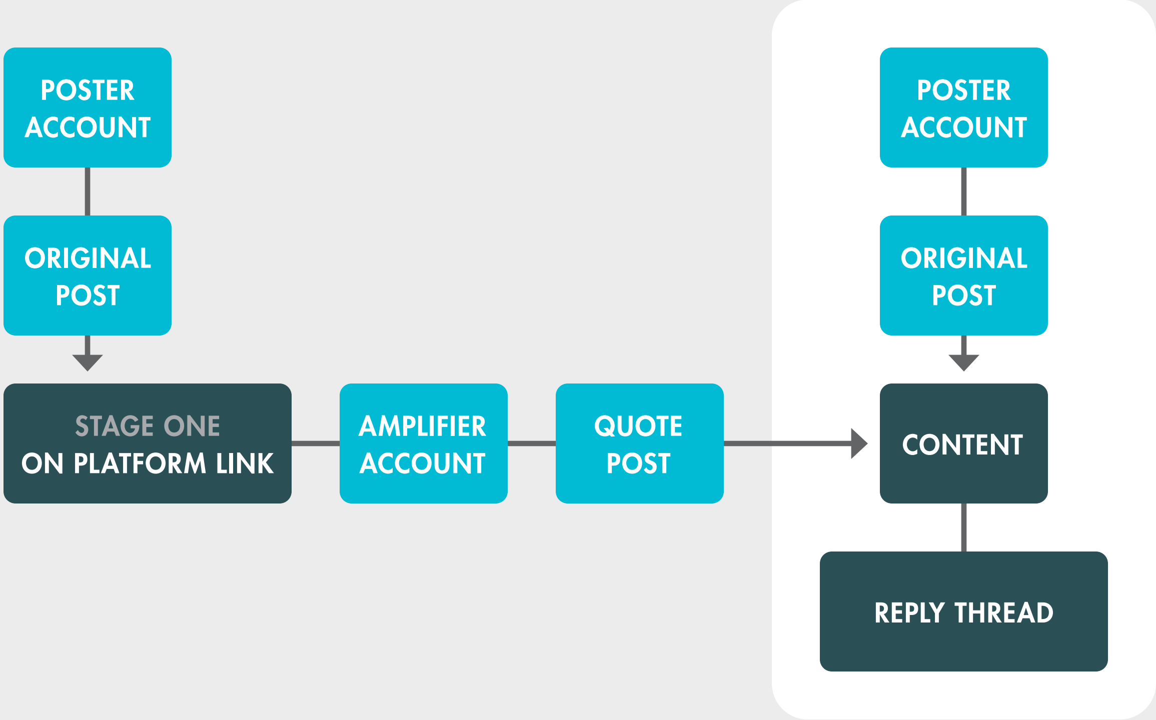
https://x[.]com/AadyaGrinn61295/status/1758285409136861315

https://www[.]reuters.com/world/biden-issue-order-targeting-jewish-settler-violence-wbank-politico-2024-02-01/

The Invisible Ink Technique

Unlike the accounts reported in previous investigations, a distinct larger set of amplifier accounts used the **Invisible Ink technique, quote posting other assets' content** with no additional text, to amplify "poster" account content in reply threads while obfuscating normal indicators of network coordination that would quickly trigger detection.

By only posting a specific tweet URL, **investigators must have each individual tweet in order to query the X API and obtain accounts**. Keywords are absent from the posts themselves, making it nearly impossible to uncover without identifying a small subset of poster accounts.



Invisible Ink Technique

A "poster account's" original post is amplified by an "amplifier account," which shares the post in a quote post in an existing reply thread started by a non-network user.

Like other techniques used in Russian information operations, Invisible Ink is likely designed to make it difficult to uncover the operations activities without knowing where to look. It allows the operation to **maintain plausible deniability, operating covertly and without declaring ties to any entity**, authentic or otherwise.

Positioning posts as replies in conversation threads **potentially increased their visibility**, prompting other users in the conversation to open the post with notification of a reply. However, these posts attracted little organic engagement. While the amplifier accounts inauthentically amplified the posts by sharing them thousands of times in quote posts to increase visibility, their quote posts did not attract any noteworthy organic engagement.

Similarly to the behaviors observed, the narratives amplified via Invisible Ink both overlapped with previously-reported Doppelgänger assets and introduced new content. The accounts and domains in this operation amplified the following key narratives in advancement of Russian interests:

Alethea observed the operation continuing to make use of clones of mainstream news sources in a variety of languages, along with their own original domains. Users reached these domains via a series of four redirects, bringing them to the final pro-Russian content.

- We identified an **IP address used for multiple stage two domains** that is assigned to a company registered in the United Kingdom; we assess with moderate confidence that this is a shell company, and have not yet found any evidence that the company exists aside from the business registration and IP assignment.
- We also identified **at least one stage two domain that appears to have been compromised**; its original U.S.-based owner is still the active registrant with no lapse shown in renewals, but Alethea does not suspect that this person is involved in the operation in any fashion.

This investigation into Doppelgänger revealed another probable connection to Russia's main military intelligence service, commonly known as the GRU. Invisible Ink accounts linked to Observateur Continental and EuroBRICS, disinformation sites with covert links to InfoRos, a Russian news agency that controls a large number of overtly and covertly-affiliated domains used to push disinformation.[5] [6] Both the US and EU have sanctioned InfoRos for engaging in influence operations. In a press release announcing these sanctions in April, 2021, **the U.S. Department of Treasury explicitly reported that the GRU's 72nd Main Intelligence Information Center controls InfoRos**, and added additional sanctions in April, 2022 to various members of its leadership.[7] [8] In July, 2023, the Council of the EU sanctioned InfoRos as an entity associated with the "Recent Reliable News" operation, which has been assessed by Recorded Future as part of Doppelgänger.[9] [10] Recent reporting based on leaked documents has indicated a link to the office of the Russian president.[11] We do not view this as ruling out potential GRU involvement, instead that Doppelgänger supports multiple lines of influence efforts by the Russian government.

[5] https://www.disinfo[.]eu/publications/how-two-information-portals-hide-their-ties-to-the-russian-news-agency-inforos/

[6] https://www.wired[.]com/story/russia-ukraine-taylor-swift-disinformation/

[7] https://home.treasury[.]gov/news/press-releases/jy0126

[8] https://home.treasury[.]gov/news/press-releases/jy0628

[9] https://www.consilium.europa[.]eu/en/press/press-releases/2023/07/28/information-manipulation-in-russia-s-war-of-aggression-against-ukraine-eu-lists-seven-individuals-and-five-entities/

[10] https://therecord[.]media/france-accuses-russians-of-impersonating-french-government-media-misinformation

[11] https://www.washingtonpost[.]com/world/2024/02/16/russian-disinformation-zelensky-zaluzhny/

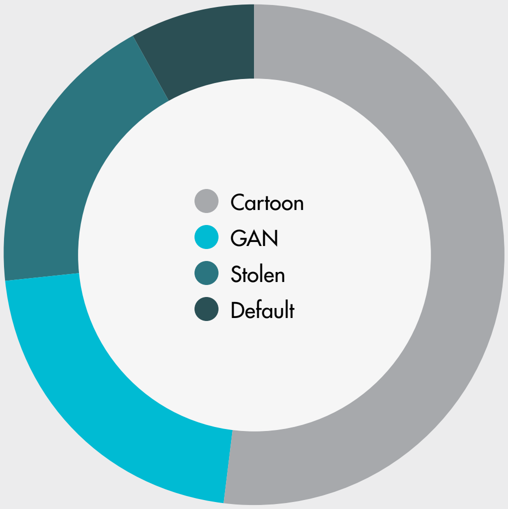
About the Network

The Accounts

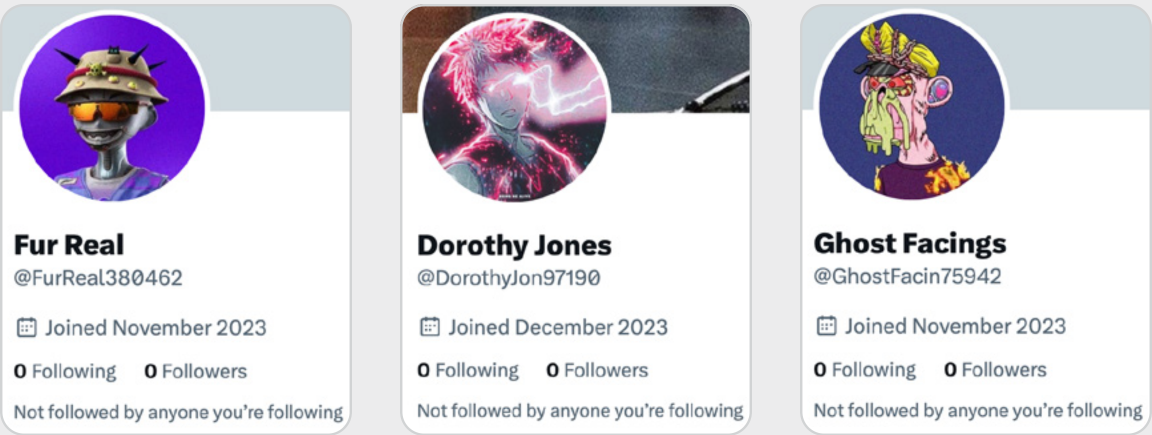
Alethea analyzed 2,129 accounts within the initial batch created since November 2023, for which 2,087 remain active and 42 have been suspended. We assess that most, if not all, of these accounts are inauthentic based on their characteristics described below. **Of these accounts, only 258 published original posts on their profile.** The accounts in this batch mentioned a total of 61,119 other accounts and published at least 310,734 posts. Many of the URLs shared by this set of accounts were no longer active at the time of this investigation. As part of our analysis of the initial batch of accounts, Alethea identified a second set of 2,260 accounts exhibiting similar behavior and notably sharing active links. **We expect to find many more accounts participating in Invisible Ink-like behavior in our future research into Doppelgänger. As of February 28, 2024, a large number of the first batch of accounts appear to have been suspended since the start of Alethea's investigation.**

We attribute the initial batch of 2,129 accounts (2,087 of which are still active) with high confidence to Doppelgänger, the characteristics of which were suggestive of distinct clusters of accounts. **Nearly all these accounts were unmistakably inauthentic, often without any steps taken to make them appear otherwise.** Signs of inauthenticity included a lack of original posts, with the majority of accounts only ever replying to other users, not liking posts, not having any followers or following any other accounts, or profile pictures that were often cartoon images (52%). This also included "Bored Ape" images and anime characters, GAN-generated pictures of people (22%), or pictures taken from other sources (19%), such as the green Android robot.

Account Profile Picture Types



Breakdown of Network Account Profile Pictures by Type



Fur Real
@FurReal380462
Joined November 2023
0 Following 0 Followers
Not followed by anyone you're following

Dorothy Jones
@DorothyJon97190
Joined December 2023
0 Following 0 Followers
Not followed by anyone you're following

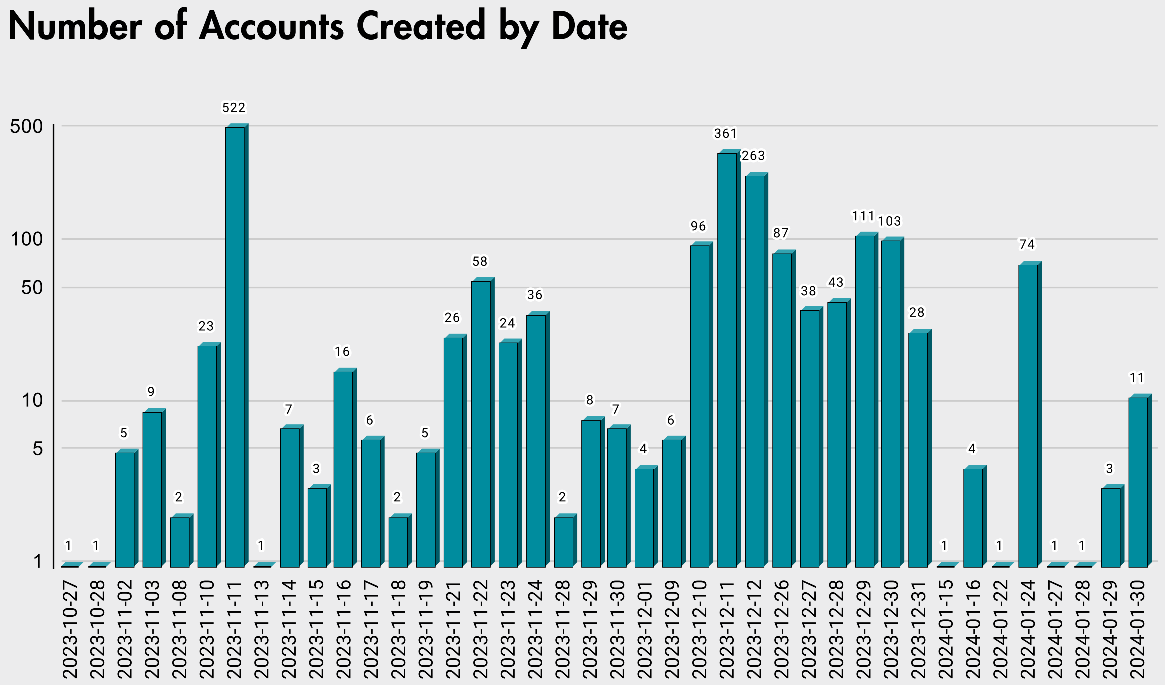
Ghost Facings
@GhostFacin75942
Joined November 2023
0 Following 0 Followers
Not followed by anyone you're following

These assets contain examples of cartoon, anime, and "Bored Ape" profile images.

Some of the accounts did attempt to create a veneer of authenticity by posting a few inane original posts, sometimes reposting crypto content, or just posting a single original post saying "hello." Another tactic used—likely to appear more authentic or otherwise evade detection—was the use of crypto spamming behaviors; as crypto accounts tend towards more spam-style behaviors normally, it is possible that the actor is hoping to avoid notice for even egregiously inauthentic behavior by blending into a sea of suspicious accounts.

Most accounts' user and display names followed a fairly specific naming convention. They combined a Western-sounding first and last name, most often a conventionally female first name, with numbers appended to the end for the usernames. When creating a new account, X automatically generates a username based on the display name and adds a string of numbers at the end, and the person creating the account can manually change this format. Exceptions to this pattern include a number of accounts that mentioned NFT/Crypto in their usernames, and others where the display name differed wildly from the username, such as accounts that also promoted the Manta Network.

The creation dates of the 2,087 active accounts in this analysis were also indicative of inauthentic activity. At least 88% (1,845) of the 2,087 accounts were created in batches of 25 or more, and 65% (1,360) were created in batches of 100 or more. On some dates, hundreds of accounts were created. For example, 545 accounts (26%) had a creation date within the 24-hour



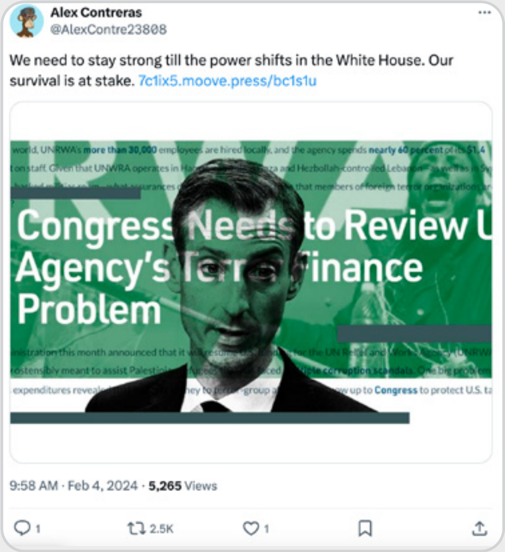
Batch Account Creations

period beginning November 10, 2023, at 21:10 UTC. We observed that many of the accounts created on the same date shared similar characteristics, such as profile photo type.

Another sign of inauthenticity was the exclusive use of Twitter Web App to post content; all content posted by the assets was done through Twitter Web App, without any use of mobile clients or third-party automation software such as Crowdfire. **This implies that they are automating the official web client for X, as the network's rapid post cadence would almost certainly necessitate some form of automation.**

Account Behaviors

Accounts behaviors varied among the profile types. **Alethea identified two major categories: posters and amplifiers.** Poster accounts shared original content directly to their timelines. This content included videos, sometimes with a text caption, or links that obscured their intended destination. As shown in the example below, posts with external links to cloned sites often included an image to look like a preview of a non-obscured external link to an article. Notably, in past reporting on domain obfuscation in Doppelgänger, the image was an actual thumbnail preview for the link, and the link appeared within the thumbnail rather than in the body text of the post.[12]



Alex Contreras
@AlexContre23808

We need to stay strong till the power shifts in the White House. Our survival is at stake. 7c1ix5.moove.press/bc1s1u

9:58 AM · Feb 4, 2024 · **5,265** Views

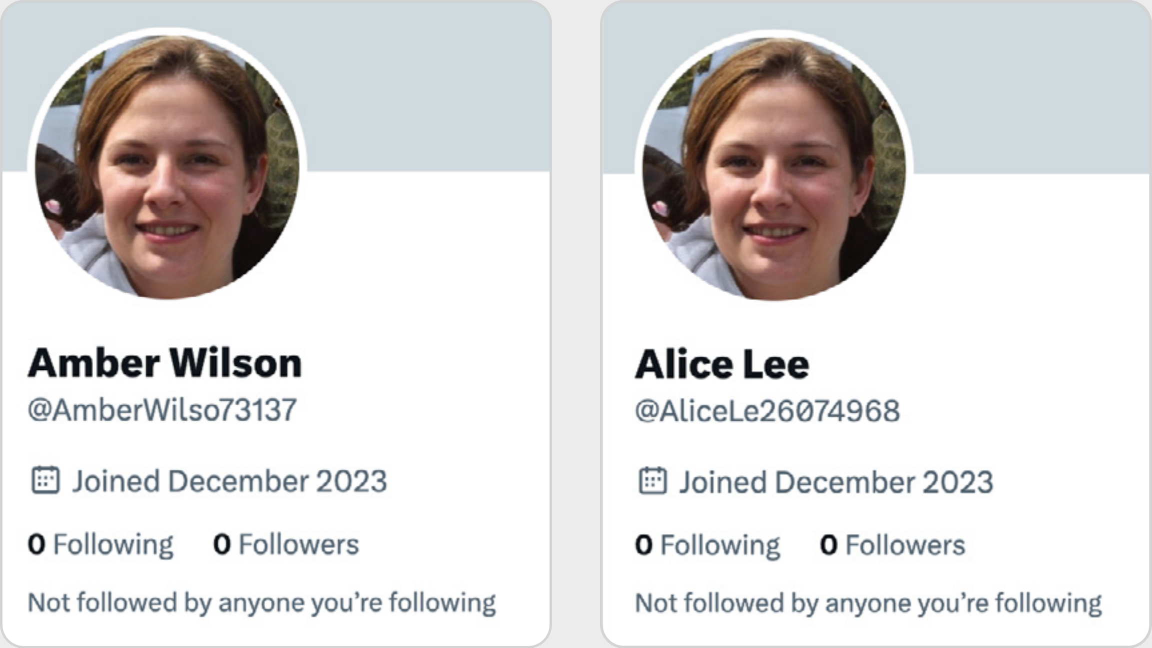
Despite its likeness to image previews embedded in X posts for external links, the image in this post was manually appended to the post.

https://twitter[.]com/AlexContre23808/status/1754157496208375984

The poster accounts rarely shared original content more than a handful of times; almost always less than ten and most posted only once or twice. The posts were then amplified by other accounts via **Invisible Ink**. The links to original posts were then shared in replies by the amplifier accounts without any additional text; X considers this type of post to be a quote post, which are counted as reposts. We assess that the hundreds or even thousands of reposts received by many of these posts were quote posts shared by amplifiers within the network. **By posting in this fashion, a search for the original text using the X API will only return the original post and not the multitude of replies.**

A second element of amplifier accounts' behavior is a tendency to reply within a thread; instead of responding to the first post, assets typically respond to another user's reply within a thread. **While this limits the post's potential visibility and thus engagement, it may also serve to assist in evading detection.**

[12] https://go[.]recordedfuture.com/hubfs/reports/ta-2023-1205.pdf



Amber Wilson
@AmberWilso73137

Joined December 2023

0 Following **0** Followers

Not followed by anyone you're following

Alice Lee
@AliceLe26074968

Joined December 2023

0 Following **0** Followers

Not followed by anyone you're following

On multiple occasions, assets had matching profile photos. These two accounts were created less than 24 hours apart.[13] [14]

The assets replied to a wide variety of accounts, with most of these replies occurring with some sense of reason or context; for example, content regarding Ukraine was often posted as a reply to Ukrainian users or news outlets. Analyzing the users to which amplifiers most commonly replied revealed some targets of the operation; five of the top 10 most replied-to users focused on news about Ukraine, with three of those specifically focused on Odessa. One stock and crypto trading account (@sharkdad81) appeared as the sixth most replied to account, while an account focused on shingles research (@ShinglesFacts) was the eighth. One Russia-based account, Alexei Palchun|Z (@palchun),

ACCOUNT	REPLIES
Odessa_Novosti	336
rogue_corq	329
lady_is_odessy	269
weather_odessa	258
BrettOdesa	255
sharkdad81	247
palchun	214
ShinglesFacts	212
SchadDeb	210
dendnepro	204

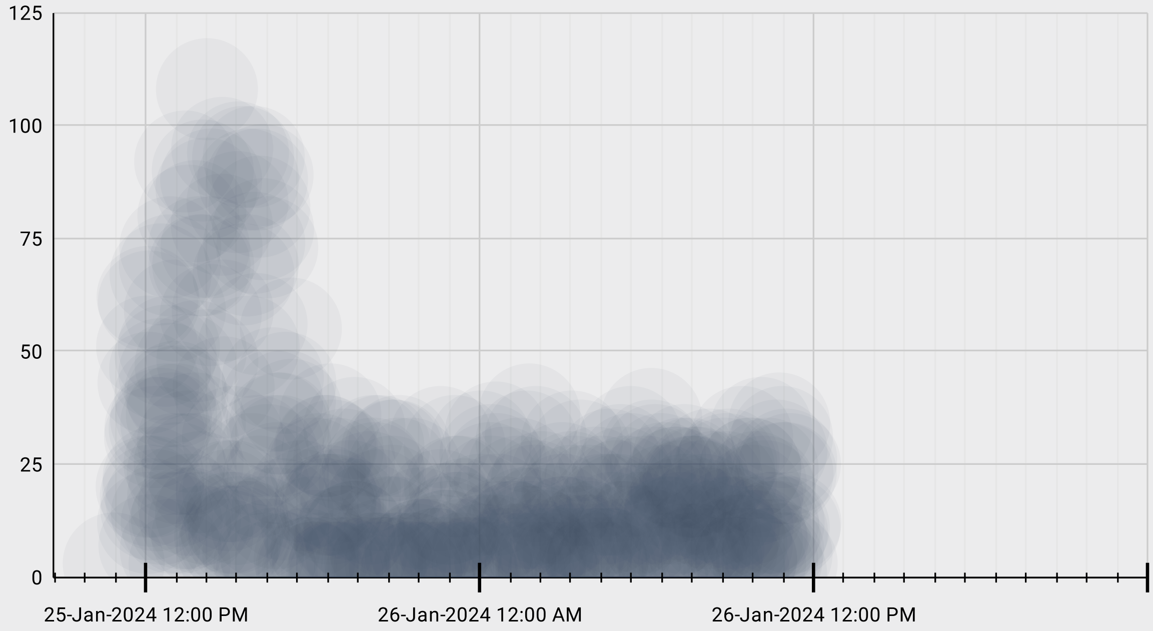
[13] https://twitter[.]com/amberwilso73137
[14] https://twitter[.]com/alicele26074968

was the seventh most replied-to account; per its API, X withheld this account in Germany due to a legal request, possibly indicating involvement in prior Russian disinformation operations.

The reason the operation chose to reply to these specific accounts is unclear, though it could indicate target audiences. For instance, replying to the account focused on shingles, a disease more common in older people, could indicate that the actor was hoping for older audiences to see their content.

These quote-post replies were clearly conducted in a automated fashion; Alethea analyzed reposts of three identical Ukrainian-language posts published at exactly 15:51 GMT on January 25, 2024. Beginning at 17:02 GMT, these posts accumulated thousands of reposts. All three accounts have since been suspended. Based on the data Alethea collected prior to these suspensions, the original posts had received 8,881 reposts by 16:10 UTC January 26, 2024. Many accounts reposted the same post multiple times to different users.

Number of Reposts by Time of Repost



Reposts by time showing rapid reposts followed by an abrupt end to the behavior

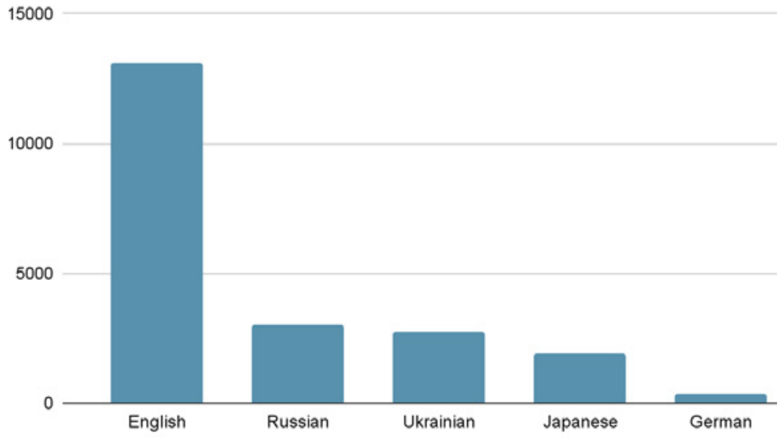
Narratives and Content

The poster accounts publishing original content on their feeds pushed specific narratives about politics in the United States, Germany, Ukraine, or France. In general, these posts pushed conservative views about 1) current political issues, especially elections; 2) military aid to Ukraine and Israel; and 3) foreign policy toward the Middle East. The topics of the threads in which the amplifier accounts replied in **Invisible Ink** sometimes overlapped with those discussed by poster accounts, especially with regard to narratives undermining Ukraine.

Amplifier accounts used Invisible Ink in conversations in different languages, including English, French, German, and Ukrainian. Oftentimes, the content of their posts, particularly videos in Ukrainian, did not correspond to the language or subject of the thread to which they responded.

While investigations into other information operations have revealed that coordinated efforts targeted both sides of the political spectrum to polarize target audiences, we observed that these accounts only shared content consistent with right-wing politics in their target country.[15]

Top 5 Languages by Post Volume

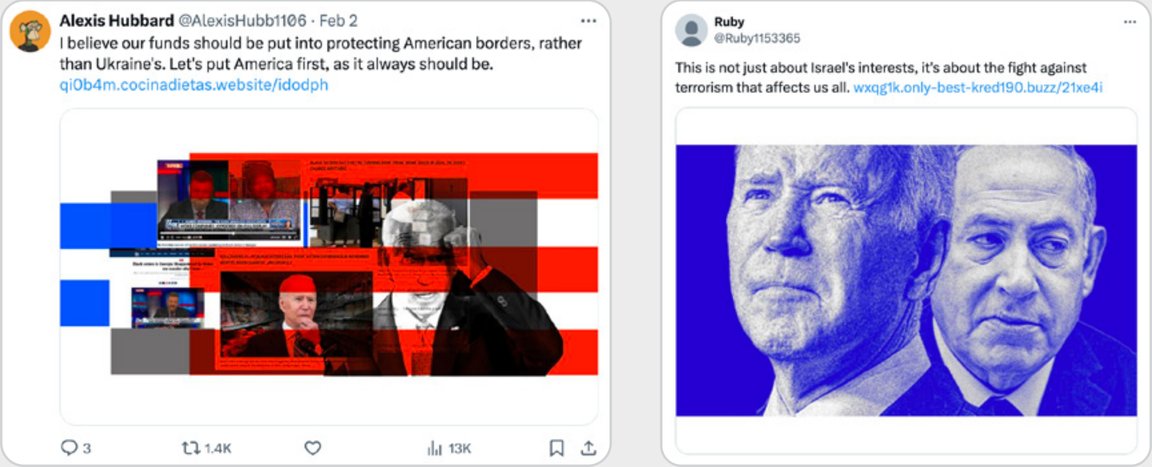


While the majority of posts in the network were published in English, over 14 total languages were used within the network.

[15] https://www.intelligence.senate[.]gov/sites/default/files/documents/The-IRA-Social-Media-and-Political-Polarization.pdf

English-Language Poster Accounts

At least 50 accounts shared original posts in English about U.S. domestic and foreign policy containing images and external links. **The most common narratives were critical of President Biden and the Democratic Party in particular, aid to Ukraine, and U.S. involvement in the Middle East.** Many of the posts used the first person, presumably in an attempt to convey an authentic American persona. This included references to the U.S. military as "our" military and a "force dedicated to our nation's protection," or stating that "we need to stay strong till the power shifts in the White House."[16] [17]



Alexis Hubbard @AlexisHubb1106 · Feb 2

I believe our funds should be put into protecting American borders, rather than Ukraine's. Let's put America first, as it always should be. qi0b4m.cocinadietas.website/idodph

Ruby
@Ruby1153365

This is not just about Israel's interests, it's about the fight against terrorism that affects us all. wxqg1k.only-best-kred190.buzz/21xe4i

On the left, an asset comments on U.S. immigration policy and aid to Ukraine, using the first person to suggest they are an American. On the right, another shares a post about the Israel-Hamas war, also in the first person, along with a link to a cloned version of Walla! News. Neither of these images returned matches from reverse image search, suggesting they are original to this network.

Despite the fact that a majority of these accounts had zero followers and only published one or two total posts, the posts consistently received approximately 1,300 or 2,600 reposts and over 5,000 views. We assess with high confidence that **the imbalance between their followership and engagement is the result of**

[16] https://x[.]com/AlexContre23808/status/1754157496208375984
[17] https://x[.]com/Alexandria33837/status/1753499311202005056

inauthentic amplification based on their uniform rates of reposting.

The accounts that posted in English played into conservative narratives about hot button issues in American politics. For example, one post asserted that aid to Ukraine and Israel would be better spent securing the southern U.S. border.[18] Another claimed that funds would “be better spent on improving domestic issues” than on “Zelenskyy’s endless demands.”[19] More generally, one account lamented that “trying to be the world’s Big Brother” had created a “budget crisis” in the United States.[20] Others generally claimed that Democrats were leading the country “down a dangerous path” or that President Biden’s immigration policies and response to the Israel-Hamas conflict had jeopardized his reelection.[21] [22]

In terms of foreign policy, one account alleged that Democrats were pursuing an “anti-Israeli agenda” and “want[ed] Hamas to win.”[23] Another user wrote, “this is not just about Israel’s interests,” but also “the fight against terrorism that affects us all,” sharing an image of President Biden and Israeli President Benjamin Netanyahu.[24] Notably, this post, though written in English, contained a link that successfully redirected to a cloned version of the Hebrew-language news site Walla! News. Reverse image searching did not reveal any matches to the image in the post. Others criticized Ukrainian President Zelenskyy’s leadership or claimed that Russia was working toward peace in the Middle East, while the U.S. was driving more conflict.[25] [26] [27] [28]

[18] https://x[.]com/AlexisHubb1106/status/1753499132059156680
[19] https://x.com/Nora63217745626/status/1758139589636583553
[20] https://x[.]com/AlexanderB87956/status/1753499705550451130
[21] https://x[.]com/AlejandroA37679/status/1753499367359602820
[22] https://x.com/AliciaJack3963/status/1753499011187609793
[23] https://x[.]com/AlexandraT33611/status/1754157351177802193
[24] https://x[.]com/Ruby1153365/status/1758139438494867908
[25] https://x[.]com/Alexandria33837/status/1754157668220956944
[26] https://x[.]com/AlexisLee179883/status/1753500123814859128
[27] https://x[.]com/AlexandraD20820/status/1753500025605210174
[28] https://x[.]com/AlexisLee179883/status/1754158187194773695

Mixed-Language Poster Accounts

At least five accounts shared original posts in a mix of English, French, German, and Ukrainian. These users published between 4 and 12 total posts. As of March 11, 2024, these accounts are suspended. **Like the other accounts, these posts targeted both domestic and foreign policy issues and received high engagement relative to their followership.** One post in Ukrainian discussed the reported rift between President Zelenskyy and General Valerii Zaluzhnyi while attempting to discredit Zelenskyy's leadership.[29] The same account also posted in German supporting Alternative for Germany (AfD) voters' "right to have their political beliefs."[30] A similar account uploaded an image of the EU and Ukrainian flags alongside the text "war never leads to prosperity" in English, while another declared former President Trump a man of peace in French.[31] [32] These accounts also raised the issue of military aid to Ukraine, claiming in English that the latest package "raises serious questions" about the use of U.S. taxpayer dollars.[33] Another complained in German that each country should pay a "fair share" of NATO contributions.[34]

[29] https://x[.]com/amaris_far77478/status/1750195104415977977

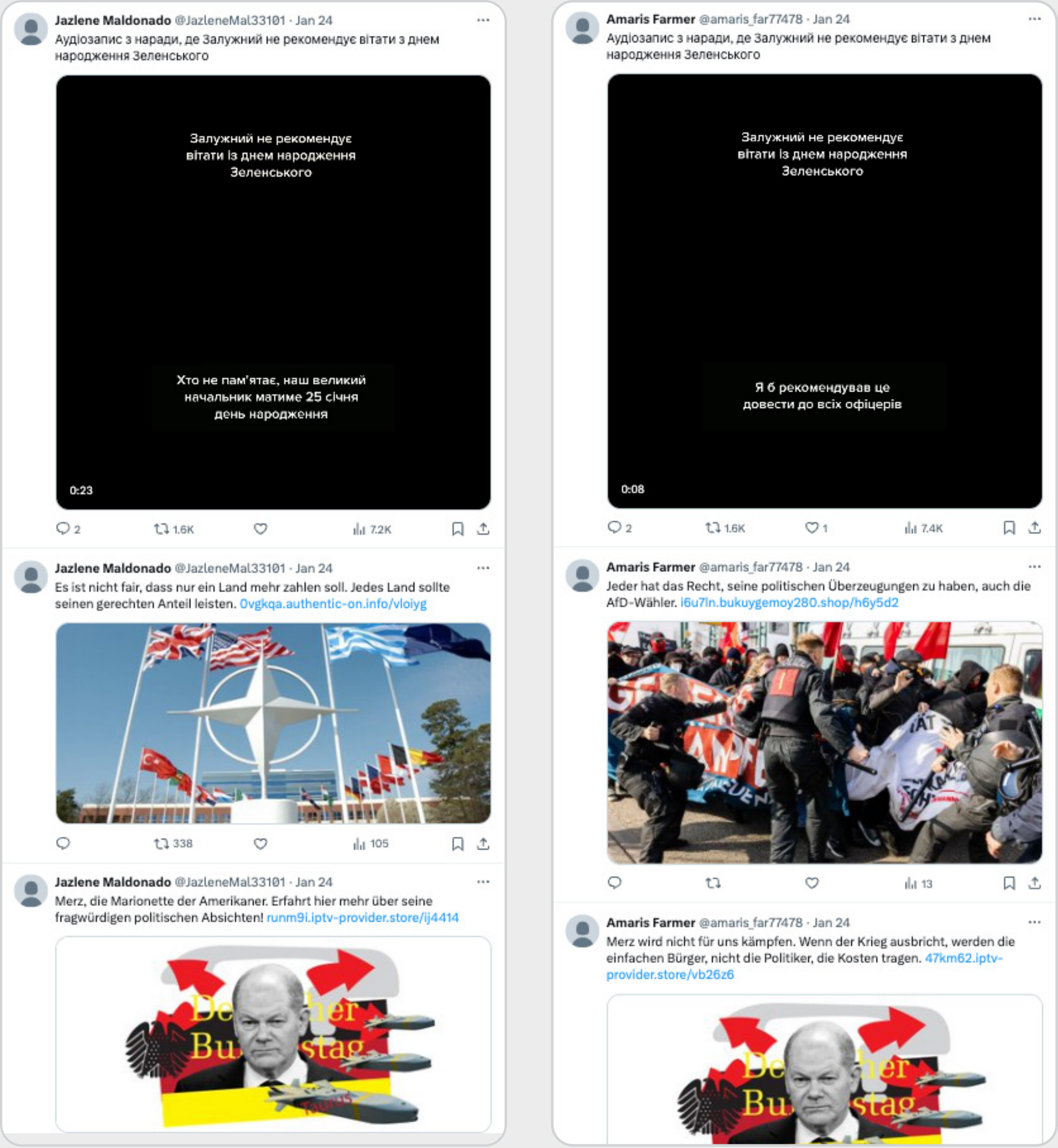
[30] https://x[.]com/amaris_far77478/status/1750166129153056779

[31] https://x[.]com/DUmnise50304/status/1747272339379904875

[32] https://x[.]com/DurocherH51789/status/1746174120977432795

[33] https://x[.]com/DurocherH51789/status/1747272314054742057

[34] https://x[.]com/JazleneMal33101/status/1750166338834764168



Jazlene Maldonado @JazleneMal33101 · Jan 24

Аудіозапис з наради, де Залужний не рекомендує вітати з днем народження Зеленського

Залужний не рекомендує вітати із днем народження Зеленського

Хто не пам'ятає, наш великий начальник матиме 25 січня день народження

Jazlene Maldonado @JazleneMal33101 · Jan 24

Es ist nicht fair, dass nur ein Land mehr zahlen soll. Jedes Land sollte seinen gerechten Anteil leisten. 0vgkqa.authentic-on.info/vloiyg

Jazlene Maldonado @JazleneMal33101 · Jan 24

Merz, die Marionette der Amerikaner. Erfahrt hier mehr über seine fragwürdigen politischen Absichten! runm9i.iptv-provider.store/ij4414

Amaris Farmer @amaris_far77478 · Jan 24

Аудіозапис з наради, де Залужний не рекомендує вітати з днем народження Зеленського

Залужний не рекомендує вітати із днем народження Зеленського

Я б рекомендував це довести до всіх офіцерів

Amaris Farmer @amaris_far77478 · Jan 24

Jeder hat das Recht, seine politischen Überzeugungen zu haben, auch die AfD-Wähler. i6u7ln.bukuygemoy280.shop/h6y5d2

Amaris Farmer @amaris_far77478 · Jan 24

Merz wird nicht für uns kämpfen. Wenn der Krieg ausbricht, werden die einfachen Bürger, nicht die Politiker, die Kosten tragen. 47km62.iptv-provider.store/vb26z6

Two accounts sharing content in Ukrainian, German, French, and English published posts—an identical pair with a video in Ukrainian and a pair of identical images of Friedrich Merz, Party leader of the Christian Democratic Union of Germany, with slightly different text—on January 24, 2024 at the same minute with one post between them.[35] [36] [37] [38]

[35] https://x[.]com/amaris_far77478/status/1750195104415977977

[36] https://x[.]com/JazleneMal33101/status/1750165583297974350

[37] https://x[.]com/amaris_far77478/status/1750165595910287824

[38] https://x[.]com/JazleneMal33101/status/1750165583297974350

German-Language Amplifier Accounts

At least 17 accounts used Invisible Ink to amplify content in German. While the majority of Invisible Ink activity amplified Ukrainian-language videos, this small subset of accounts engaged in this behavior by replying to threads with quote posts containing text and an image, similar to the format of those published by English-language accounts. **These posts criticized German foreign policy, foreign aid spending, and other political parties in favor of the conservative AfD party.** They claimed the "Traffic Light" coalition has ruined [Germany's] economy," called for its replacement, and accused "pro-American eco-parties" of "endangering" Germany's economy.[39] [40] Supporting the position of AfD, one user called on viewers to support farmers in their protests against the cost of environmental regulations targeting agricultural pollution.[41] [42] Adding to these complaints about the economy, the same account asserted that Friedrich Merz was prioritizing aid to Ukraine while ignoring Germany's "economic crisis."[43]

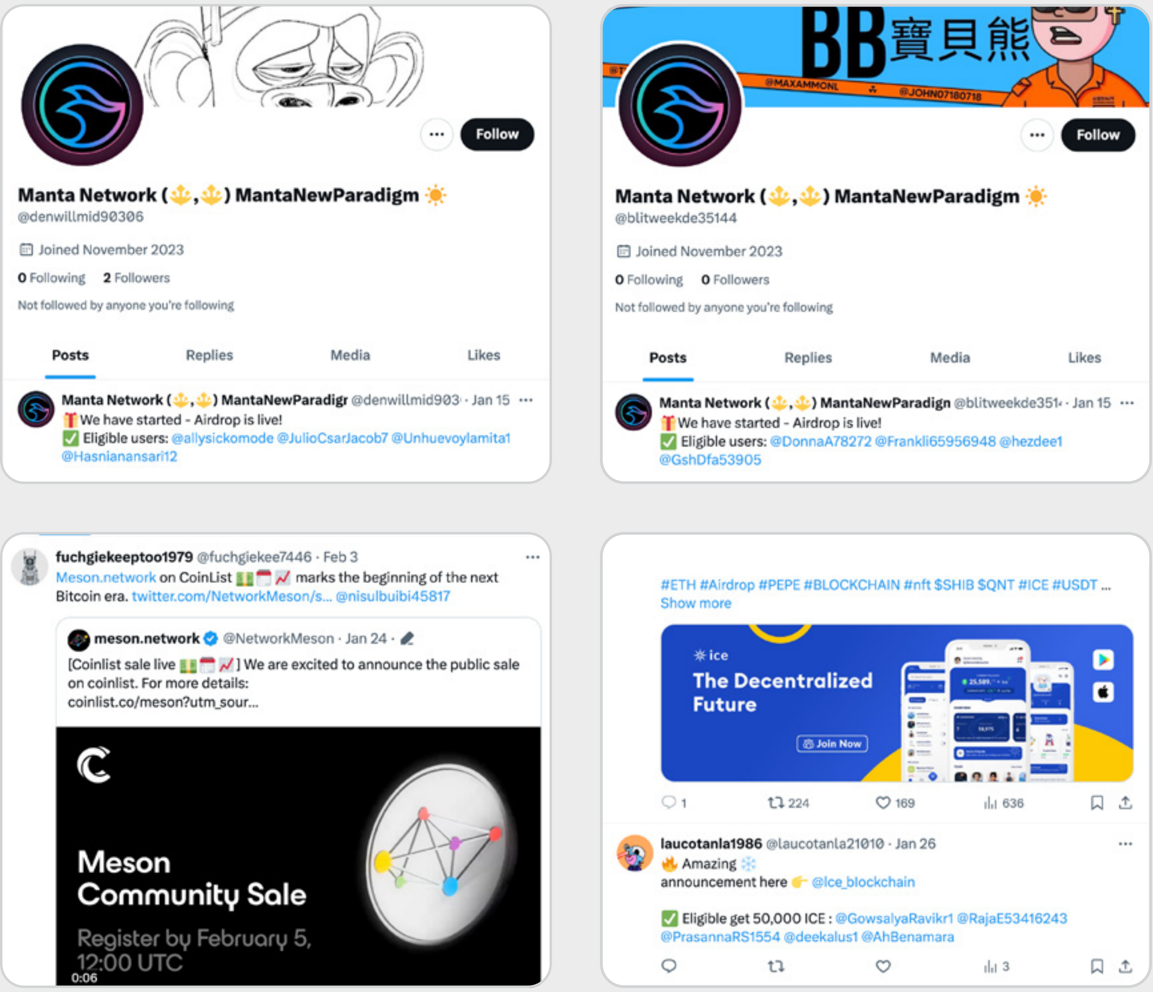
Echoing the English-language posts, German-language content attempted to undermine Ukraine's legitimacy or dissuade support for military aid. Posts broadly suggested that the German government should stop serving foreign interests and take care of its own, echoing the English-language post referenced in the previous section.[44] Others were more direct, urging Germany to change its foreign policy to improve relations with Russia or lamenting that "corruption continues to thrive in Ukraine."[45] [46]

Apolitical Crypto Amplifier Accounts

Approximately 6% of accounts (129) were designed to look like promoters of cryptocurrencies or crypto aficionados. **We assess with high confidence that they were not compromised accounts due to their shared creation dates with other batches of accounts in the network.** Many of the accounts posted about

[39] https://x[.]com/CainDarien32236/status/1748361823751975304
[40] https://x[.]com/GavynBaraj28992/status/1748417371386094024
[41] https://x[.]com/huffman_je54693/status/1748719910937587766
[42] https://www[.]theguardian.com/environment/2024/jan/15/why-europe-farmers-are-protesting
[43] https://x[.]com/EugeneN23848/status/1748460496527728764
[44] https://x[.]com/IrwinLizet64086/status/1748360991694344611
[45] https://x[.]com/ruthe282466/status/1728867908070371368
[46] https://x[.]com/CassandraA31051/status/1748360154439905353

cryptocurrencies, used Invisible Ink to amplify videos in Ukrainian, and then returned to sharing content about cryptocurrencies. The accounts promoted otherwise legitimate crypto and blockchain assets, such as the Manta Network (MANTA) and Meson Network, using branding and images from their official accounts' X posts.



Manta Network (🔱,🔱) MantaNewParadigm ☀️
@denwillmid90306

Joined November 2023

0 Following **2** Followers

Not followed by anyone you're following

Posts Replies Media Likes

Manta Network (🔱,🔱) MantaNewParadigr @denwillmid903 · Jan 15 ···
🎁 We have started - Airdrop is live!
✅ Eligible users: @allysickomode @JulioCsarJacob7 @Unhuevoylamita1 @Hasniananasari12

Manta Network (🔱,🔱) MantaNewParadigm ☀️
@blitweekde35144

Joined November 2023

0 Following **0** Followers

Not followed by anyone you're following

Posts Replies Media Likes

Manta Network (🔱,🔱) MantaNewParadign @blitweekde351 · Jan 15 ···
🎁 We have started - Airdrop is live!
✅ Eligible users: @DonnaA78272 @Frankli65956948 @hezdee1 @GshDfa53905

fuchgiekeeptoo1979 @fuchgiekee7446 · Feb 3 ···
Meson.network on CoinList 💵📅📈 marks the beginning of the next Bitcoin era. twitter.com/NetworkMeson/s... @nisulbuibi45817

meson.network @NetworkMeson · Jan 24 ·
[Coinlist sale live 💵📅📈] We are excited to announce the public sale on coinlist. For more details: coinlist.co/meson?utm_sour...

#ETH #Airdrop #PEPE #BLOCKCHAIN #nft $SHIB $QNT #ICE #USDT ...
Show more

1 224 169 636

laucotanla1986 @laucotanla21010 · Jan 26 ···
🔥 Amazing ❄️
announcement here 👉 @Ice_blockchain

✅ Eligible get 50,000 ICE : @GowsalyaRavikr1 @RajaE53416243 @PrasannaRS1554 @deekalus1 @AhBenamara

3

Examples of accounts promoting the "Manta Network," "Meson Network," and "$ICE" cryptocurrency that also shared videos in Ukrainian in reply posts.

One possible explanation for this account behavior is that it was a test of the viability of accounts posing as cryptocurrency promoters. For example, mixing the Invisible Ink content with other posts and reposts **promoting cryptocurrencies**

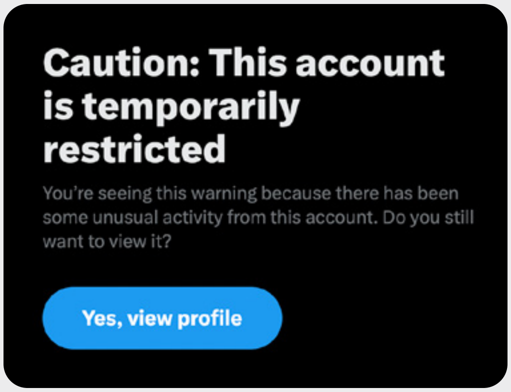
may have been an attempt to avoid restriction and suspension for suspicious account activity.

Japanese Language Accounts

Most of the 14 accounts operating in Japanese have already been suspended by X, and the accounts that are still active typically have a similar profile picture of a checkmark. These users collectively published at least 1,800 posts, but only shared reposts and reply posts, refraining from publishing any original content. Like the accounts promoting crypto, these accounts amplified Ukrainian-language content using Invisible Ink in between sharing Japanese-language reposts.

Platform Actions

As the amplifier accounts make little to no effort to hide their inauthenticity, they have been regularly suspended by likely automated enforcement systems on X. This leaves content from poster accounts intact for longer with substantial numbers of reposts—numbering in the hundreds to thousands—while reposting amplifier accounts are suspended and easily replaced. Alethea was only able to capture the reposting behavior for the Ukrainian-language posts described below; all others that were reviewed seem to have had the amplifier accounts suspended.



Caution: This account is temporarily restricted

You're seeing this warning because there has been some unusual activity from this account. Do you still want to view it?

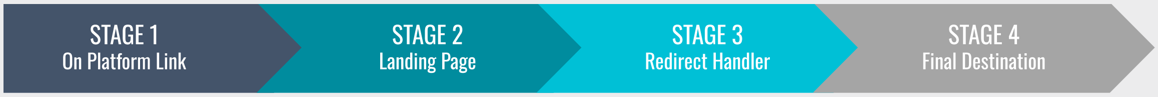
Restricted warning applied to 2,004 of the 2,087 accounts analyzed

Additionally, the vast majority of all accounts Alethea analyzed were temporarily restricted due to their behavior, necessitating an additional click for an end user to see the accounts and their content. This restriction is likely part of automated enforcement measures taken against potentially inauthentic accounts and it limits the visibility of the account's content, meaning that fewer users would see the posts, without notifying the owner. **During the course of this analysis, Alethea observed that some accounts which were previously restricted are now suspended.**

Website and Network Activity

A well-known element of Doppelgänger activity is their titular use of cloned or otherwise fake websites. The accounts analyzed by Alethea continued this trend, posting links that led users through three stages of redirects before landing at a final fake website. Alethea's investigation into the domains—along with previous reporting—suggests that the actors tailor this behavior to geographic regions likely using smart redirections; for instance, specific countries such as but not limited to France, Germany, the U.K., and the U.S. would be routed through the redirect chain. However, countries such as Mexico and Hong Kong, for example, would be stopped at stage two, the landing page.[47]

The redirect chain is a four-stage process when all the right conditions are met. The first stage link is posted by seed accounts which would redirect the user through the second stage link of a recently acquired or possibly compromised domain. The stage two link, referred to as the landing page, communicates with a stage three domain, which Alethea will refer to as the "redirect handler." The redirect handler determines the stage four link based on information supplied from the landing page. The stage four link is the final destination and is intended for the user that clicked the link on the platform.



STAGE 1
On Platform Link

- Posted by seed bot accounts on platform.
- Reposted by amplifying bot accounts on platform.
- User clicks and goes through the stages or is redirected to bing.com.

STAGE 2
Landing Page

- Landing page domains were previously owned/active.
- Hosted base64 encoded JavaScript calls to the redirect handler with campaign data.

STAGE 3
Redirect Handler

- Receives campaign data which determines the final destination.
- Hosted JavaScript extracts the final destination site and then launches the site using the Document Object Model (DOM).

STAGE 4
Final Destination

- User lands at a doppelgänger or a website with pro-Russian ideology.

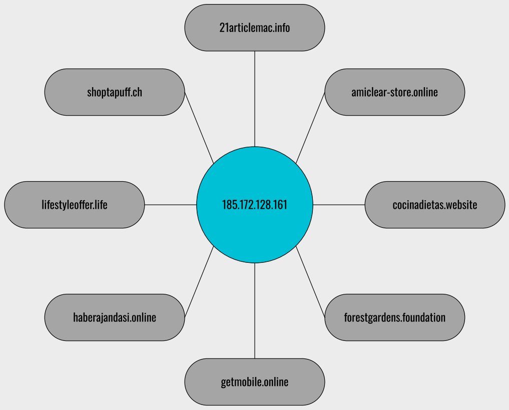
The flowchart above describes the stages of the redirect chain taking users from a poster account's original X post through to the final Doppelgänger news site.

[47] https://www.disinfo[.]eu/wp-content/uploads/2022/09/Doppelganger-1.pdf

IP Address and Domain Overview

The main IP address investigated was 185.172.128.161 due to its high communication seen by stage one links. **Based on a WHOIS data search, Alethea assesses with high confidence that this IP is controlled by Russian entities.** The IP shows a history of Russian linkage and its latest record shows that it's associated with a company called TNSECURITY LTD with an address of 124 City Road, London UK EC1V 2NX and domain tnsecurityl[.]ltd.

Upon investigating the company TNSECURITY LTD, the company was allegedly created in the U.K. by an individual named Berezina Anastasjia, who is supposedly a 19-year-old Latvian citizen. At the time of writing this report, Alethea has not found evidence that this person has any other online presence.[48] The only other use of the name appears on a second U.K. business filing for a web development and marketing company—Bluejetlag LTD—which also has no web or social media presence.[49] The domain, tnsecurityl[.]ltd, redirects to tnsecurity[.]ca, which appears to be owned and operated by a person named Terry Nusyna, a Canadian citizen who appears to be unrelated or unwitting to the operation.



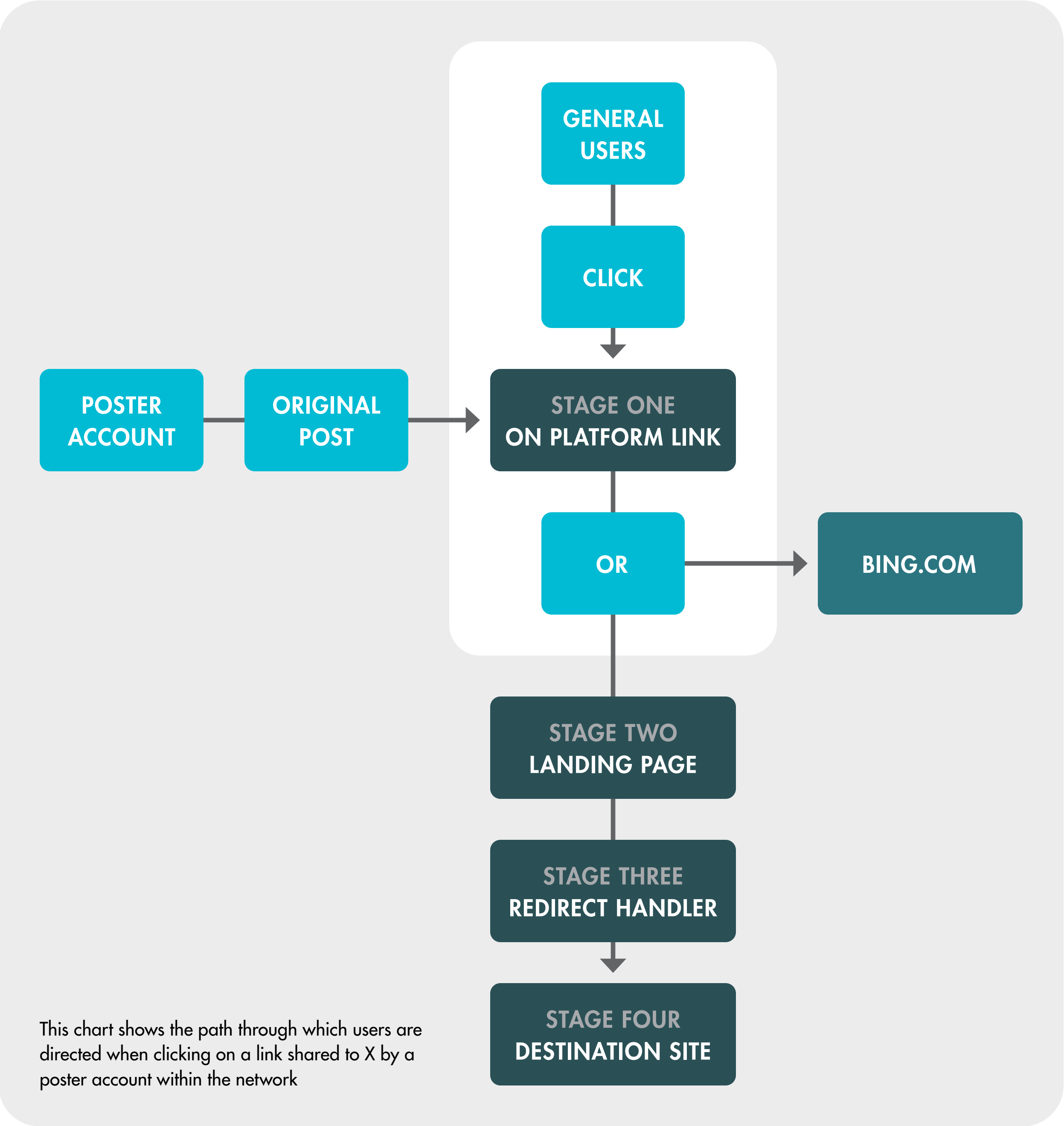
Stage one domains connected to IP address: 185.172.128.161

There are four notable domains that were analyzed:

- scuolavela[.]ch; Stage 1 // posted on platform by seed account
- kiddosdeals[.]com; Stage 2 // resold domain
- sdgqaef[.]site; Stage 3 // redirect handler
- electionwatch[.]live; Stage 4 // final destination

[48] https://www.onlinefilings.co[.]uk/people/officers/search/312926100001/

[49] https://suite.endole.co[.]uk/insight/company/14942686-bluejetlag-limited



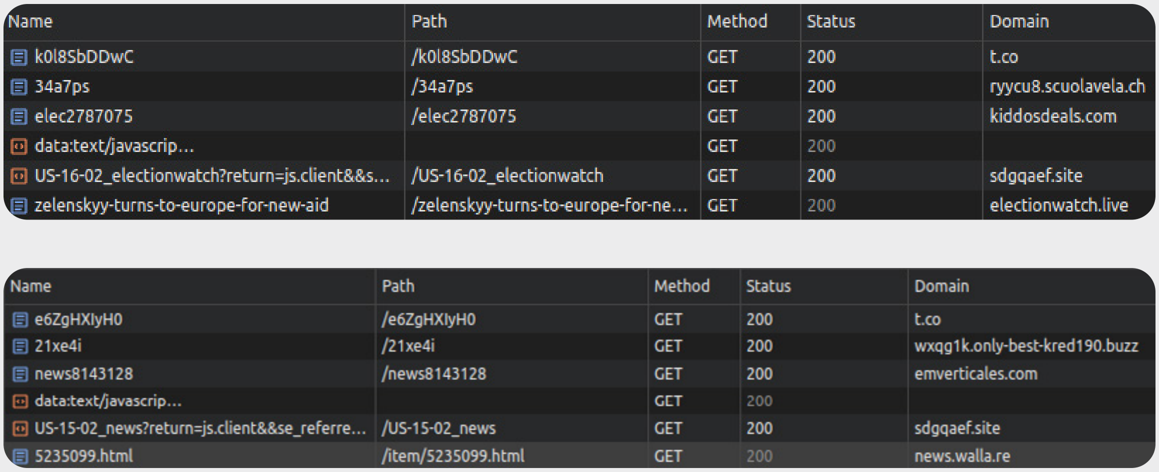
This chart shows the path through which users are directed when clicking on a link shared to X by a poster account within the network

Links posted on the platform by a seed account are considered stage one. When clicked on by a user, the user would be redirected through stages two and three unknowingly before arriving at stage four, the final destination.

Stage two domains appeared to include compromised domains based on the WHOIS history that was seen along with data observed in Wayback. The purpose of these domains was to send campaign data to the redirect handler, a stage three domain, which could be used to track the actor's influence operations.

The stage three domain acts as the redirect handler which depends on data received from a stage two domain. At this stage, the redirect handler parses through JavaScript code, specifically where the location object exists within the headers. The location object houses the stage four link.

A stage four domain is the final destination. This is where a user ends up after clicking on a stage one domain. The stage four domains are the copycat sites portraying pro-Russia information to a user.

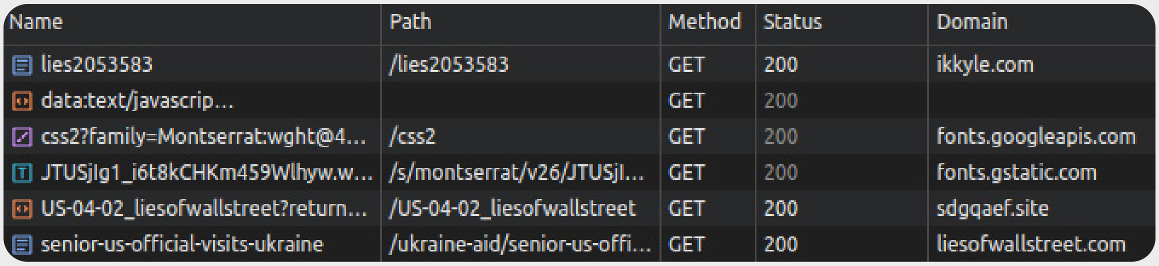


Name	Path	Method	Status	Domain
k0l8SbDDwC	/k0l8SbDDwC	GET	200	t.co
34a7ps	/34a7ps	GET	200	ryycu8.scuolavela.ch
elec2787075	/elec2787075	GET	200	kiddosdeals.com
data:text/javascrip…		GET	200	
US-16-02_electionwatch?return=js.client&&s…	/US-16-02_electionwatch	GET	200	sdgqaef.site
zelenskyy-turns-to-europe-for-new-aid	/zelenskyy-turns-to-europe-for-ne…	GET	200	electionwatch.live

Name	Path	Method	Status	Domain
e6ZgHXlyH0	/e6ZgHXlyH0	GET	200	t.co
21xe4i	/21xe4i	GET	200	wxqg1k.only-best-kred190.buzz
news8143128	/news8143128	GET	200	emverticales.com
data:text/javascrip…		GET	200	
US-15-02_news?return=js.client&&se_referre…	/US-15-02_news	GET	200	sdgqaef.site
5235099.html	/item/5235099.html	GET	200	news.walla.re

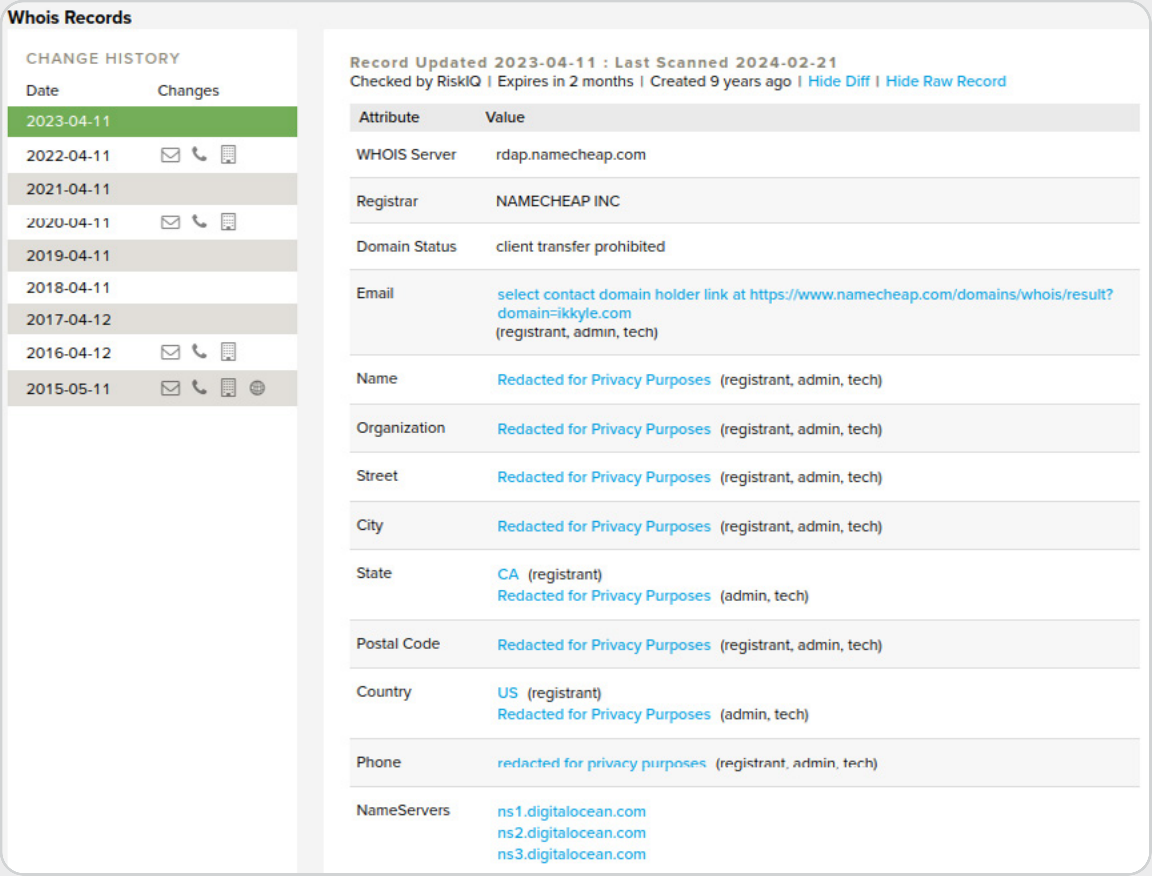
Two different redirect flows from original links to the stage four Doppelgänger sites

The landing page, ikkyle[.]com, appears to be a compromised domain based on consecutive WHOIS historical registration dates with the registrant information still tied to the state of California. Further investigation into the domain on Wayback shows historical pages of crypto information which may be linked to Doppelgänger accounts seen promoting stage one links. Furthermore, a historical screenshot on DomainTools shows the domain as a Doppelgänger of seaworldabudhabi.com, which may indicate possible testing related to their infrastructure or operation.



Name	Path	Method	Status	Domain
lies2053583	/lies2053583	GET	200	ikkyle.com
data:text/javascrip...		GET	200	
css2?family=Montserrat:wght@4...	/css2	GET	200	fonts.googleapis.com
JTUSjIg1_i6t8kCHKm459Wlhyw.w...	/s/montserrat/v26/JTUSjI...	GET	200	fonts.gstatic.com
US-04-02_liesofwallstreet?return...	/US-04-02_liesofwallstreet	GET	200	sdgqaef.site
senior-us-official-visits-ukraine	/ukraine-aid/senior-us-offi...	GET	200	liesofwallstreet.com

Redirect flow of ikkyle[.]com starting from Stage Two



Whois Records

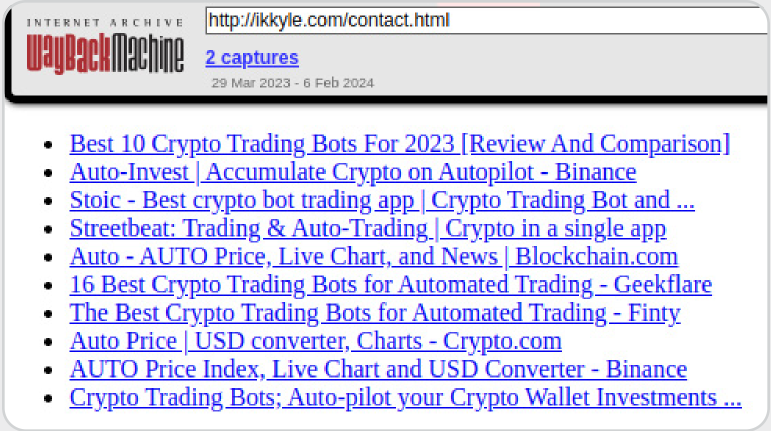
CHANGE HISTORY

Date	Changes
2023-04-11	
2022-04-11	✉ ☎ 🏢
2021-04-11	
2020-04-11	✉ ☎ 🏢
2019-04-11	
2018-04-11	
2017-04-12	
2016-04-12	✉ ☎ 🏢
2015-05-11	✉ ☎ 🏢 🌐

Record Updated 2023-04-11 : Last Scanned 2024-02-21
Checked by RiskIQ | Expires in 2 months | Created 9 years ago | Hide Diff | Hide Raw Record

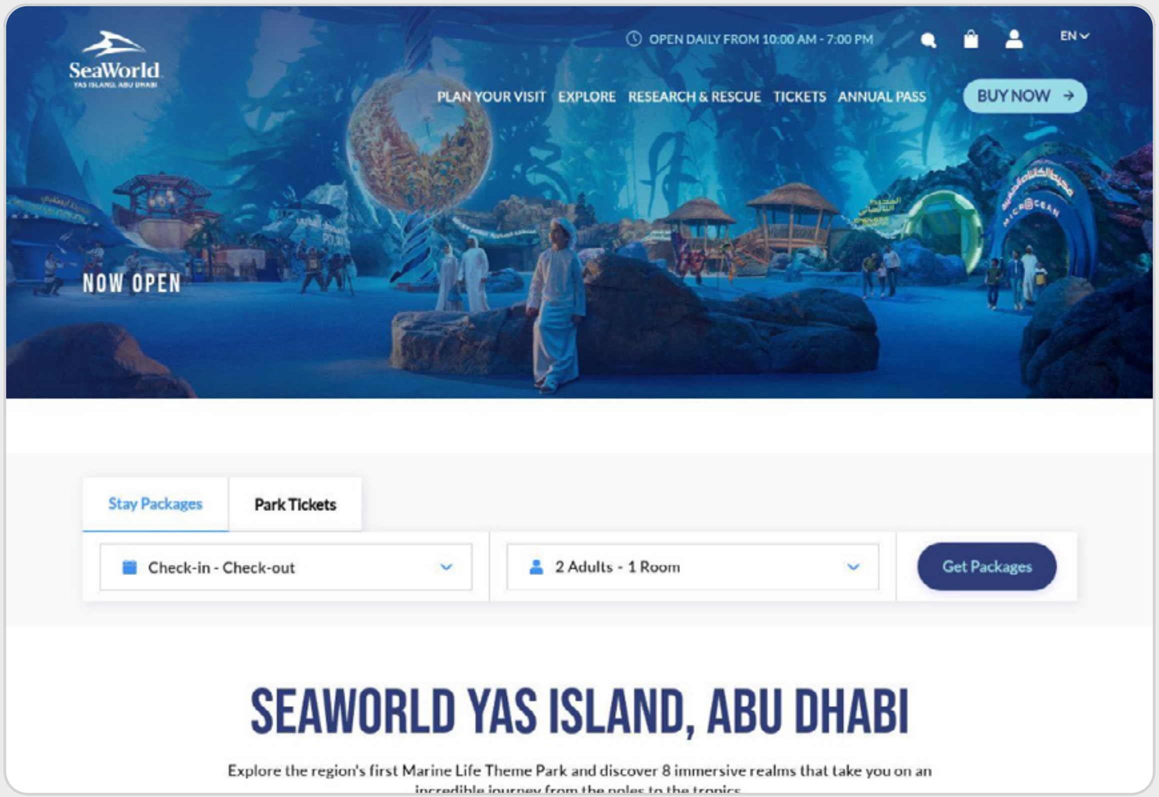
Attribute	Value
WHOIS Server	rdap.namecheap.com
Registrar	NAMECHEAP INC
Domain Status	client transfer prohibited
Email	select contact domain holder link at https://www.namecheap.com/domains/whois/result?domain=ikkyle.com (registrant, admin, tech)
Name	Redacted for Privacy Purposes (registrant, admin, tech)
Organization	Redacted for Privacy Purposes (registrant, admin, tech)
Street	Redacted for Privacy Purposes (registrant, admin, tech)
City	Redacted for Privacy Purposes (registrant, admin, tech)
State	CA (registrant) Redacted for Privacy Purposes (admin, tech)
Postal Code	Redacted for Privacy Purposes (registrant, admin, tech)
Country	US (registrant) Redacted for Privacy Purposes (admin, tech)
Phone	redacted for privacy purposes (registrant, admin, tech)
NameServers	ns1.digitalocean.com ns2.digitalocean.com ns3.digitalocean.com

Ikkyle[.]com WHOIS change history



- Best 10 Crypto Trading Bots For 2023 [Review And Comparison]
- Auto-Invest | Accumulate Crypto on Autopilot - Binance
- Stoic - Best crypto bot trading app | Crypto Trading Bot and ...
- Streetbeat: Trading & Auto-Trading | Crypto in a single app
- Auto - AUTO Price, Live Chart, and News | Blockchain.com
- 16 Best Crypto Trading Bots for Automated Trading - Geekflare
- The Best Crypto Trading Bots for Automated Trading - Finty
- Auto Price | USD converter, Charts - Crypto.com
- AUTO Price Index, Live Chart and USD Converter - Binance
- Crypto Trading Bots; Auto-pilot your Crypto Wallet Investments ...

https://web.archive.org/web/20230329023906/http://ikkyle.com/contact.html

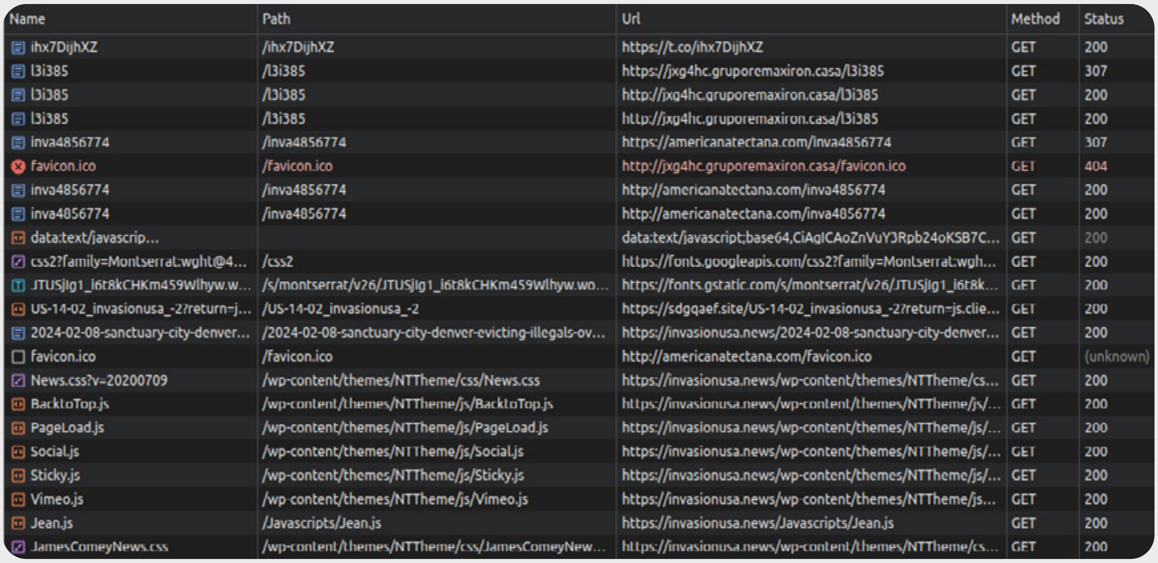


SEAWORLD YAS ISLAND, ABU DHABI

Explore the region's first Marine Life Theme Park and discover 8 immersive realms that take you on an incredible journey from the poles to the tropics

DomainTools historical screenshot of ikkyle[.]com as of 2023-09-28

Alethea observed an additional behavior not previously reported in connection with Doppelgänger. **In addition to linking to their own cloned sites, we found one instance of their original posts linking to invasionusa[.]news, a site affiliated with the Natural News family of websites.** Natural News, founded in 2008 by U.S.-based Michael Allen Adams, has previously been accused of spreading disinformation, most often anti-vaccination content.[50] Alethea assesses with moderate confidence that this was simply a target of opportunity and that the content Natural News produced simply aligns with Russian messaging, and we did not observe any evidence to suggest that Natural News is wittingly participating in the Doppelgänger operation, or otherwise cooperating with the Russian government.



Name	Path	Url	Method	Status
ihx7DijhXZ	/ihx7DijhXZ	https://t.co/ihx7DijhXZ	GET	200
l3i385	/l3i385	https://jxg4hc.gruporemaxiron.casa/l3i385	GET	307
l3i385	/l3i385	http://jxg4hc.gruporemaxiron.casa/l3i385	GET	200
l3i385	/l3i385	http://jxg4hc.gruporemaxiron.casa/l3i385	GET	200
inva4856774	/inva4856774	https://americanatectana.com/inva4856774	GET	307
favicon.ico	/favicon.ico	http://jxg4hc.gruporemaxiron.casa/favicon.ico	GET	404
inva4856774	/inva4856774	http://americanatectana.com/inva4856774	GET	200
inva4856774	/inva4856774	http://americanatectana.com/inva4856774	GET	200
data:text/javascrip...		data:text/javascript;base64,CiAgICAoZnVuY3Rpb24oKSB7C...	GET	200
css2?family=Montserrat:wght@4...	/css2	https://fonts.googleapis.com/css2?family=Montserrat:wgh...	GET	200
JTUSjIg1_i6t8kCHKm459Wlhyw.w...	/s/montserrat/v26/JTUSjIg1_i6t8kCHKm459Wlhyw.wo...	https://fonts.gstatic.com/s/montserrat/v26/JTUSjIg1_i6t8k...	GET	200
US-14-02_invasionusa_-2?return=j...	/US-14-02_invasionusa_-2	https://sdgqaef.site/US-14-02_invasionusa_-2?return=js.clie...	GET	200
2024-02-08-sanctuary-city-denver...	/2024-02-08-sanctuary-city-denver-evicting-illegals-ov...	https://invasionusa.news/2024-02-08-sanctuary-city-denver...	GET	200
favicon.ico	/favicon.ico	http://americanatectana.com/favicon.ico	GET	(unknown)
News.css?v=20200709	/wp-content/themes/NTTheme/css/News.css	https://invasionusa.news/wp-content/themes/NTTheme/cs...	GET	200
BacktoTop.js	/wp-content/themes/NTTheme/js/BacktoTop.js	https://invasionusa.news/wp-content/themes/NTTheme/js/...	GET	200
PageLoad.js	/wp-content/themes/NTTheme/js/PageLoad.js	https://invasionusa.news/wp-content/themes/NTTheme/js/...	GET	200
Social.js	/wp-content/themes/NTTheme/js/Social.js	https://invasionusa.news/wp-content/themes/NTTheme/js/...	GET	200
Sticky.js	/wp-content/themes/NTTheme/js/Sticky.js	https://invasionusa.news/wp-content/themes/NTTheme/js/...	GET	200
Vimeo.js	/wp-content/themes/NTTheme/js/Vimeo.js	https://invasionusa.news/wp-content/themes/NTTheme/js...	GET	200
Jean.js	/Javascripts/Jean.js	https://invasionusa.news/Javascripts/Jean.js	GET	200
JamesComeyNews.css	/wp-content/themes/NTTheme/css/JamesComeyNew...	https://invasionusa.news/wp-content/themes/NTTheme/cs...	GET	200

Screenshot showing the redirect path leading to invasionusa[.]news, part of the Natural News network of websites

[50] https://www.isdglobal[.]org/wp-content/uploads/2020/06/20200620-ISDG-NaturalNews-Briefing-V4.pdf

Overlap with Prior Doppelgänger Activity and Other Russian IO

Alethea assesses that this network is almost certainly affiliated with the Doppelgänger information operation and is also affiliated with the GRU because of the following elements:

- One of the accounts Alethea analyzed posted a link whose fourth stage resolution was electionwatch[.]live, a previously observed and attributed Doppelgänger domain.[51]
- Domains that Alethea investigated as part of the redirect chain were also previously attributed by Recorded Future as affiliated with Doppelgänger, including ggspace[.]space, mypride[.]press, electionwatch[.]live, and tribunalukraine[.]info.
- Alethea also observed that the Doppelgänger domain ggspace[.]space previously redirected to observateurcontinental[.]fr, which was attributed to the GRU.[52]

Additionally, a small piece of overlap with known APT28/GRU infrastructure was found. Investigation of two stage four domains—lepoint[.]foo and walla[.]re—shows overlap with infrastructure known to be used by APT28/Fancy Bear.[53] Specifically, in the WHOIS history we found the use of 1337 Services, a subsidiary of Njalla, based in Saint Kitts and Navis.

[51] https://go.recordedfuture[.]com/hubfs/reports/ta-2023-1205.pdf

[52] https://www.disinfo[.]eu/publications/how-two-information-portals-hide-their-ties-to-the-russian-news-agency-inforos/

[53] https://threatconnect[.]com/blog/using-fancy-bear-ssl-certificate-information-to-identify-their-infrastructure/

Alethea