AUGUST 2024

SECOND QUARTER

Adversarial Threat Report

Margarita Franklin, Director, Public Affairs, Security
Mike Torrey, Security Engineer
David Agranovich, Security Policy Director, Threat Disruption
Mike Dvilyanski, Head of Threat Investigations

Meta

TABLE OF CONTENTS

PURPOSE OF THIS REPORT

Our public threat reporting began over six years ago when we first shared our findings about coordinated inauthentic behavior (CIB) by a Russian covert influence operation linked to the Internet Research Agency (IRA). Since then, we have expanded our ability to respond to a wider range of adversarial behaviors as global threats have continued to evolve. To provide a more comprehensive view into the risks we tackle, we've also expanded our threat reports to include insights into other threats, as part of our quarterly reporting. In addition, we're also publishing threat indicators to contribute to the security community's efforts to detect and counter malicious activity across the internet (see Appendix).

We expect the make-up of these reports to continue to change in response to the changes we see in the threat environment in different areas. This report is not meant to reflect the entirety of our security enforcements, but to share notable trends and investigations to help inform our community's understanding of the evolving threats we see. We welcome ideas from our peers to help make these reports more informative.

For a quantitative view into our enforcement of our Community Standards, including content-based actions we've taken at scale and our broader integrity work, please visit Meta's Transparency Center here: https://transparency.fb.com/data/.

What is Coordinated Inauthentic Behavior or CIB?

We view CIB as coordinated efforts to manipulate public debate for a strategic goal, in which fake accounts are central to the operation. In each case, people coordinate with one another and use fake accounts to mislead others about who they are and what they are doing. When we investigate and remove these operations, we focus on behavior, not content — no matter who's behind them, what they post or whether they're foreign or domestic.

Continuous CIB enforcement: We monitor for efforts to come back by networks we previously removed. Using both automated and manual detection, we continuously remove accounts and Pages connected to networks we took down in the past. See the Doppelganger section for details on our approach to persistent threats.

KEY INSIGHTS

We're sharing threat research into six new covert influence operations from Russia, Vietnam and the United States. We detected and removed many of these cross-internet campaigns early in their audience building efforts. We also include an update on Doppelganger, the most persistent Russian influence operation. Finally, as we look ahead to a number of elections including in the US, we're sharing some key insights into the global threat landscape and what we expect to see through the rest of this year.

Use of GenAI by threat actors

We continue to monitor and assess the risks associated with evolving new technologies like AI. Our findings so far suggest that GenAI-powered tactics provide only incremental productivity and content-generation gains to the threat actors, and have not impeded our ability to disrupt their influence operations. We continue to assess that our industry's defense strategies, including our focus on behavior (rather than content) in countering adversarial threat activity, already apply and appear effective at this time. Here are some examples of what we've seen to date:[1]

- A deceptive campaign from Russia published a large volume of stories resembling authentic articles from across the internet, including mainstream media, on its fictitious 'news' websites. We assess that these stories were likely summaries of the originals generated using AI tools to make them appear more unique.
- The same campaign also posted AI-generated news-reader videos on YouTube.
- They also ran fictitious journalist personas, each with consistent profile photos across the internet, often GAN-created (generative adversarial networks), to appear more convincing. This continues a trend we've been monitoring since 2019.
- Doppelganger used AI-generated images, likely as part of its effort to create unique visuals to avoid automated detection at scale.
- Finally, the same campaign appeared to rely on AI tools to generate posts and translate its content, as was reported publicly here and here.

Top global source of CIB: key takeaways

Russia remains the number one source of global CIB networks we've disrupted to date since 2017, with 39 covert influence operations. The next most frequent sources of foreign interference are Iran, with 30 CIB networks, and China, with 11.

Here are some trends that stood out to us in Russian campaigns:

THEMATIC FOCUS

Earlier Russia-origin operations varied significantly in the narratives they focused on – from culture wars to social hot-button issues and the operators' business interests in the countries they

[1] Our previous updates on the risks and opportunities enabled by GenAI can be found here, and here.

targeted. Since the start of Russia's full-scale war in 2022, they have largely consolidated around undermining Ukraine at home and abroad, though some networks also focused on other countries in Russia's immediate neighborhood like Georgia, Moldova and others. No matter who the operators are, the narrative across different networks is shared: supporting Ukraine's government in its defense against Russia is detrimental for both Ukraine and its allies.

→ **Takeaways**: Between now and the US elections in November, we expect Russia-based operations to promote supportive commentary about candidates who oppose aid to Ukraine and criticize those who advocate for aiding its defenses. This could take the shape of blaming economic hardships in the US on providing financial help to Ukraine, painting Ukraine's government as unreliable, or amplifying voices expressing pro-Russia views on the war and its prospects.

FOR-HIRE OPERATORS

New commercial entities continue to appear behind Russia-based influence operations. These for-hire campaigns, operated by contractors (rather than security agencies themselves, as we saw in the past), have continued to run low-quality, high-volume efforts, making errors including in their operational security. In fact, we continue to see real people calling these networks out as trolls, as they struggle to engage authentic audiences.

→ **Takeaway**: This trend will likely continue with more marketing and other firms joining deceptive campaigns in response to the demand heightened by Russia's war.

INCREASED PERSISTENCE

Past Russia-based operations, including those linked to the IRA, tended to respond to disruptions by significantly changing their tactics, techniques and procedures (TTPs). After aggressive repeated disruptions, a number of them shifted operations elsewhere on the internet or even shut down. In contrast, since 2022, the for-hire operators have shown a much stronger persistence (see our Doppelganger update). In response to detection, they keep on creating new assets over and over again, without much effort put into building audiences on social media. They do, however, appear to put extensive efforts into operating their websites, likely in an attempt to preserve their content against ongoing disruptions by social media platforms.

→ **Takeaway**: Without a concerted effort to disrupt the internet infrastructure powering these campaigns, we expect these website-centric operations to persist as long as their customers task them to do so, regardless of their efficacy.

HIGH DISCOVERABILITY AS AN ASSET

In the past, the IRA's funder, Yevgeniy Prigozhin, leveraged what we call perception hacking to gain notoriety, including by turning the IRA's failures to evade takedowns into public reporting by media outlets painting Prigozhin's efforts as omnipresent and therefore effective. The latest for-hire operations tend to be noisy at the onset, as if they want researchers and journalists to see them in the short window before they are taken down. These persistent efforts will likely provide many

opportunities to expose these attempts across the internet. However, their presence alone does not equal influence.

→ **Takeaways**: Ahead of the elections, it'll be particularly critical to report on these threats with caution to avoid amplifying them without context or evidence of impact. Overstating their influence risks undermining trust in the information environment and institutions.

CO-OPTING REAL PEOPLE

A number of recent Russian operations engaged likely witting and unwitting people to create content and amplify their campaigns, including in Armenia and Europe, in addition to earlier cases. When such coordination happens outside of our platform, it makes it challenging to identify such a link with foreign malicious campaigns so we can counter them. In addition, these operations often target journalists and public figures to get them to pick up these narratives and give them credence. This could include seeding hacked or forged materials with unwitting opinion-makers and politicians.

→ **Takeaways**: We encourage influential figures and the public at large to remain vigilant to avoid playing into the hands of deceptive operations attempting to manipulate public debate. In addition, it is important for political campaigns, candidates, public figures and media outlets to keep their information security up to date because they represent attractive targets for hackers. As part of our effort to help strengthen account security among these high-target groups, we have run a series of in-app reminders directing people to our security and safety features.

01

Russia

We removed 76 Facebook accounts, 30 Pages, and 11 accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in Russia and targeted Georgia, Armenia, and Azerbaijan.

This operation centered around fictitious news websites with distinct branding focused on the individual countries this campaign targeted. They also had a presence across several internet services, including ours, YouTube, Telegram, and TikTok to backstop these entities so they appear more legitimate and can withstand scrutiny by platforms and researchers. As of this writing, these fictitious news websites continue to operate and post "news" stories about politics in Georgian, Armenian, Azerbaijani, and Russian. In Georgia, they posted about the most recent protests against the "foreign agent law" where they criticized the protesters and supported the ruling party, Georgian Dream. In Azerbaijan, they posted about local events and criticized the West. In Armenia, they posted about politics, including supportive commentary about Russia, a former Armenian official currently detained in Azerbaijan, and criticism of the Prime Minister of Armenia.

On our apps, the individuals behind this network used fake accounts – some of which were detected and disabled by our automated systems prior to our investigation – to drive people to their off-platform websites, manage Pages, and post content. Notably, they appear to have co-opted people in Armenia to create original videos posted on TikTok, YouTube and on our apps by one of the operation's brands – the "Agora Expert Club."

We found this network as part of our internal investigation into recidivist attempts by a previously removed spammy inauthentic behavior (IB) reported to us by ISFED, a non-profit in Georgia. This earlier IB effort was basic in its tactics and targeted Facebook, TikTok, and Telegram.

Although the people behind the CIB network attempted to conceal their identity and coordination, our investigation found links to individuals associated with a Moscow-registered marketing firm called IMA Digital.

- *Presence on Facebook and Instagram:* 76 Facebook accounts, 30 Pages, and 11 Instagram accounts.
- *Followers*: About 3,800 accounts followed one or more of these Pages, and around 1,850 accounts followed one or more of these Instagram accounts.
- Ad spend: About $77,000 in spending for ads, paid for mostly in US dollars.

02

Russia

We removed 20 Facebook accounts, 14 Pages, and nine accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in Russia and targeted primarily English- and French-speaking audiences globally.

This operation centered around fictitious news websites hosted in the regions targeted. For example, a site called Euro Top News purports to be a UK-based outlet that publishes stories on international affairs under fictitious journalist bylines. Likely in an attempt to seem more authentic, it listed the address of the legitimate publication Ok!Magazine, in addition to appropriating the VAT number from an unconnected UK-based digital marketing firm.

These fictitious 'news' websites, as of this writing, continue to publish a large volume of stories that resemble authentic articles from across the internet, including by mainstream media like Fox News, Deutsche Welle, and Telegraph, but also InfoBrics, Pravda and Aydinlik, including using some of their images and even citing them as sources at times. However, we assess that these stories – which tend to be more of a summary of the originals – are likely generated using AI tools to make them appear more unique. The websites interspersed political stories with unrelated entertainment and celebrity gossip, articles from wikiHow, and other content from across the internet, likely to build an audience and ensure consistent supply of content and search engine optimization.

These fictitious news brands had presence across several internet services, including ours, YouTube, Telegram, and X (formerly Twitter) to backstop these entities and their fake contributors so they appear more legitimate and can withstand scrutiny by platforms and researchers. Each fictitious journalist persona had consistent profile photos across the internet, often GAN-created, to appear more convincing.

This operation's tactics varied across different apps. They typically posted likely AI-generated summaries with links to the fictitious 'news' websites on Telegram, and AI-generated news-reader videos on YouTube. On our apps, they usually posted links to these 'news' websites. On X, they typically posted links to fictitious 'news' sites, Telegram channels and YouTube videos.

They used fake accounts — some of which were detected by our automated systems prior to this investigation — to run Pages, post content, and drive people to the operation's off-platform websites and internet accounts.

This network appeared to be focused on two main topics. For French-speaking audiences in Francophone Africa, this operation promoted Russian integration in the region and criticized France's presence there, including through cartoon-style images. For English-speaking audiences,

this campaign posted primarily about diminishing support for Ukraine in the West, including AI-generated newsreaders on YouTube focused on criticizing US President Biden and Democrats for providing aid to Ukraine instead of investing in their own country.

We found this activity as a result of an internal investigation into suspected coordinated inauthentic behavior in the region, and removed it before it was able to build authentic audiences on our apps.

- *Presence on Facebook and Instagram:* 20 Facebook accounts, 14 Pages, and 9 Instagram accounts.
- *Followers:* About 300 accounts followed one or more of these Pages, and about 1,800 accounts followed one or more of these Instagram accounts.
- *Ads*: Around $2,800 in spending for ads, paid for mostly in US dollars.

03

Russia

We removed 43 Facebook accounts and 85 Pages for violating our policy against coordinated inauthentic behavior. This network originated in Russia and targeted primarily Ukraine, Moldova and Ukrainians living in Europe, and to a lesser extent France and Germany.

This campaign appears to be an unsuccessful attempt at a 'three-dimensional chess' campaign to undermine Ukraine while pretending to support it. On the one hand they assumed a seemingly pro-Ukraine stance by calling for more weapons from Europe, but they also highlighted Ukrainian battle casualties, called for harsher punishment for Ukrainians who avoid conscription, and demanded Presidential elections in Ukraine in 2024.

This operation failed to gain traction among authentic audiences on our apps in the short time it was active before we disrupted it. We continue to detect and block their recidivist attempts to come back.

It combined online efforts to establish fictitious news and civic entities across the internet with amplifying real-world stunts in France, Germany, and Poland related to the war in Ukraine. While we cannot confirm whether these events themselves and their online amplification were organized by the same individuals, it appears that some real-world events involved placing flyers with QR codes that led to the online operation's accounts on Telegram.

On our apps, this operation began with creating a Page for a fictitious entity called the Ukrainian European Front which was backstopped on Telegram, likely to appear more legitimate. The Page was detected and disabled by our automated systems on the same day. A few days later, the individuals behind it tried again – the new Page, too, got shut down. At this time, the first article about the Front appeared on a Polish news website, and was then picked up by a handful of press outlets primarily in Ukraine. The story described this entity as working to "prevent Europe and the entire civilized world from forgetting about Ukraine" and called for Europe to support Ukraine in its fight against "Russian dictatorship." The operation attempted to create another Front Page claiming that the previous one was shut down by "Putin's trolls." This fictitious entity claimed responsibility for some of the real-world performative actions the network tried to amplify.

In fact, amplifying claims of these offline events taking place across Europe was one of the key elements of this activity. It included posting photos and videos of: stickers placed in public areas in France and Germany claiming to show the faces of deceased Ukrainian soldiers and calling for weapons for Ukraine; graffiti near the Consulate of Ukraine in Warsaw calling for elections in

Ukraine; a stunt with an election urn in Warsaw offering a choice for President between Volodymyr Zelenskyy and Petro Poroshenko and claiming to hold similar events in other European cities.

They then used Pages purporting to be news entities to 'report' on these events as if they were authentic grassroots developments. Some of these actions, including placing coffins by the Eiffel Tower and coffin-themed graffiti in Paris to warn France against sending military personnel to Ukraine, attracted the attention of the local police and reporters. A fictitious Ukrainian art collective, Мрія (Dream), with a newly created Facebook Page, claimed responsibility for these stunts, which were quickly reported on in France.

On our apps, the individuals behind this operation used fake accounts – some of which were detected and removed prior to this investigation by our automated systems. These accounts had GAN profile photos, relied on proxy IP infrastructure to hide the operators' location and were used primarily to make this campaign's Pages appear local to the countries they targeted.

Outside of amplifying the real-world Ukraine-related events in Europe, this operation used Pages and accounts to appeal to people in Ukraine and its diaspora abroad. The people behind it posted about news and current events, including criticism of the current government for failing to defend the country, low military mobilization rates and calls to hold the Presidential election in 2024, claiming that President Zelenskyy's decision to postpone it violates Article 103 of the Constitution. They also created fan Pages for Petro Poroshenko, the former president of Ukraine, and the Ukrainian heavyweight boxer Oleksandr Usyk, advocating for each of them to run for President.

In Moldova, this campaign posted in Romanian about pro-Russian politicians and criticized the current government. It also promoted a seemingly independent petition on the Open Petition platform calling to abolish postal voting in Moldova. Finally, the operation repeatedly used its Pages to amplify TikTok videos about politics by an individual publicly reported to have been recruited by the GRU (Russia's military intelligence service) to participate in the 2023 Star of David graffiti stunt in Paris. The amplification of this graffiti on X (former Twitter) was linked to Doppelganger by the French government.

We began our investigation after investigative journalists at Le Monde contacted us about a small portion of this activity. Although the people behind it attempted to conceal their identity and coordination, our investigation found links to individuals in Russia, including some connected with people involved in numerous CIB campaigns we removed in the past by the Russian Internet Research Agency (IRA), Social Design Agency and NewsFront.

- *Presence on Facebook and Instagram:* 43 Facebook accounts and 85 Pages.
- *Followers:* About 32,000 accounts followed one or more of these Pages, including a portion of inauthentic accounts in Brazil, which suggests attempts at purchasing fake engagement to make these Pages appear more popular than they were.
- *Ads*: Around $35,000 in spending for ads, paid for mostly in US dollars with the vast majority focused on Ukraine and also Moldova.

04

Russia

We removed 12 Facebook accounts, 32 Pages, five Group and three accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in Russia and targeted primarily Ukraine, and to a much lesser extent Poland and the broader European Union and the United States.

We found two separate clusters of activity. The first was operated by a social media management group in Sri Lanka and targeted Ukraine and also Poland. The second was run by a similar entity in Nepal and targeted the EU and the US. Both clusters were primarily focused on undermining Ukraine and its support in the West.

The people behind this operation relied on fake accounts – some of which were detected and removed prior to our investigation – to manage Pages posing as Ukrainian organizations, impersonate public figures in the West including some pro-Russia commentators, and to post content. Some of these accounts used profile photos that were likely GAN-created. This operation used proxy IP addresses to appear to be based in the regions it targeted.

The primary effort targeted at Ukraine included creating a Page for what appears to be a fictitious entity: Center for Information Defense. This cluster shared long-form text posts in Ukrainian about domestic politics, conscription, claims of disinformation, and criticism of the government and President Zelenskyy.

A small effort targeted at Poland included posting in Polish about Ukrainian migrants, including suggesting that Polish schools should teach students Ukrainian language, history and literature to help Ukrainian refugees feel more comfortable in Poland.

The efforts targeted at the EU and US included posting in English primarily about Western aid provided to Ukraine, war casualties among Ukrainian soldiers, claims that Ukraine's government has failed to protect its people, and criticism of the West for providing lethal weapons to Ukraine and for allowing war crimes in Gaza. This cluster posted content copied from the public figures in the West that this operation tried to impersonate.

We began our investigation after receiving a tip from the FBI about a small portion of this activity which led our teams to find the broader network. Although the people behind it attempted to conceal their identity and coordination behind the two separate clusters run by the operators in

different countries, our investigation found links to Ruposters, a news aggregator based in Moscow, with a public history of servicing government-related contracts.

- *Presence on Facebook and Instagram:* 12 Facebook accounts, 32 Pages, 5 Group and 3 Instagram accounts.
- *Followers:* About 23,000 accounts followed one or more of these Pages, around 18,500 accounts joined one or more of these Groups, and about 280 accounts followed one or more of these Instagram accounts.
- Advertising: Around $41,000 in spending for ads, paid for mostly in Sri Lankan rupees and US dollars.

05

Vietnam

We removed 112 Facebook accounts, 65 Pages, and 49 accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in Vietnam and targeted primarily Lebanon, the US, UK, and France, and to a lesser extent Saudi Arabia and Qatar.

This activity focused primarily on criticizing Qatar and included several regional campaigns targeting multiple apps, including ours, YouTube, Telegram, and X (formerly Twitter), in addition to running websites and placing ads on billboards in the US and Lebanon.

They ran four regional campaigns. First, the English-language effort targeted the US and UK. It posted original content about Israeli hostages, called on Qatar to help their release and criticized Qatar for its investments globally. It included what appear to be AI-generated memes titled "The Qatar Plot." Second, the French-language effort targeted France. It posted about the alleged alliance between Qatar and Iran, the importance of retaining traditional French values and secularism, and criticized Shia Islam and Qatari investments in Europe. Third, the French- and Arabic-language efforts targeted Lebanon. It posted in support of Palestine, criticized Iran's involvement in the Israel-Hamas war, and called for Lebanon to avoid a repeat of the 2006 war in the region. Finally, the Arabic-language effort targeted Saudi Arabia and Qatar. It posted content similar to the French- and English-language campaigns.

In English, the individuals behind this activity operated a fictitious advocacy group called *It's In Your Hands*. In commenting on this group's billboard to the New York Post, they claimed to be "an informal coalition of Christian leaders and organizations around the world working on helping the hostage families since October." They appeared to have engaged an American celebrity to record a video plea to Sheikha Moza bin Nasser, the mother of the Emir of Qatar, to help free the Israeli hostages from Hamas. The video and a Change dot org petition were featured on this group's website. The billboard with this plea was placed in Times Square earlier this year.

In Lebanon, this operation appeared to have placed another billboard with a hashtag Lebanon_Does_Not_Want_War calling for Lebanon to abstain from military hostilities with Israel. It was reported by the local press as being "organized by a coalition of Lebanese youth and businessmen, with support from the director of an advertising company in the Arab Gulf."

On our apps, this network used fake accounts with GAN profile photos – the majority of which were detected by our automated systems prior to this investigation – to amplify this operation's efforts and manage Pages.

We found this activity as a result of our internal investigation into suspected coordinated inauthentic behavior in the region. Our analysis benefited from numerous public reports about various regional campaigns linked to this operation. Although the people behind this network attempted to conceal their identity and coordination, our investigation found links between the on-platform activity and a Vietnam-based entity called LT Media, likely running it on behalf of its customers. This firm offered services to run fake accounts and evade detection by online platforms. We issued a cease and desist letter to LT Media, demanding that they immediately stop activity that violates Meta's policies.

- *Presence on Facebook and Instagram:* 112 Facebook accounts, 65 Pages, and 49 Instagram accounts.
- *Followers:* About 38,000 accounts followed one or more of these Pages, and 0 accounts followed these Instagram accounts.
- *Ads*: Around $1.2 million in spending for ads, paid for mostly in Vietnamese dongs.

06

United States

We removed 96 Facebook accounts, 16 Pages, 12 Group, and three accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in the United States and targeted domestic audiences in the country.

It centered around a fictitious political advocacy group – the Patriots Run Project PRP – operating websites and social media accounts, including on our apps and X. These websites represented the state chapters of PRP and appealed to "real conservatives" in states like Arizona, Michigan, Nevada, Ohio, Pennsylvania, Wisconsin, and North Carolina to run "as an independent" against what they referred to as the "uniparty" with detailed step-by-step instructions on how to do so.

On our apps, this operation used fake accounts – some of which were detected and disabled by our automated systems prior to this investigation – to create fictitious personas and amplify PRP's content to make it appear more popular than it was. These accounts appeared to have been acquired from Bangladesh, with many starting out with GAN profile photos and later changing to other images. These fictitious personas attempted to maintain relative operational security (OpSec) by using proxies to pretend to be living in the particular states this campaign targeted. To seem more credible, they often interspersed the PRP-related posts with local content related to state sports teams and events, and local restaurant check-ins, in addition to political memes which they copied from other people on the internet.

The people behind this network posted in English about US elections and primaries, including criticisms of "Republican and Democrat elites", "God", "guns", and "illegal immigrants."

We found this activity as a result of our internal investigation into suspected coordinated inauthentic behavior and removed it before it was able to build an audience among authentic communities on our apps. Although the people behind it attempted to conceal their identity and coordination, our investigation found links to individuals associated with a US-based on-platform entity called RT Group.

- *Presence on Facebook and Instagram:* 96 Facebook accounts, 16 Pages, 12 Group and 3 Instagram accounts.
- *Followers:* About 1,700 accounts followed one or more of these Pages, around 1,200 accounts joined one or more of these Groups, and about 2,300 accounts followed one or more of these Instagram accounts.
- *Ads*: Around $50,000 in spending for ads, paid for mostly in US dollars.

07

Update on Doppelganger's attempts to stay afloat across the internet

As part of our ongoing transparency reporting on Doppelganger, a cross-internet influence operation from Russia, we're sharing our 8th update in 23 months that includes our latest research into this malicious activity.[2] It includes notable shifts in this operation's tactics on our platform in response to aggressive enforcement, its latest attempts at evading detection, and nearly 300 threat indicators added to our industry's largest repository of 6,000+ indicators related to this threat actor. Since our last update in May, we have also detected and removed over 5,000 accounts and Pages.

WHAT IS DOPPELGANGER?

Nearly two years ago, we were the first technology company to publicly report on Doppelganger, an operation centered around a large network of websites spoofing legitimate news outlets. The EU Disinfo Lab and the Digital Forensic Research Lab published open-source research at the same time. In December 2022, we were the first to publicly attribute it to two companies in Russia who were sanctioned by the EU in 2023 and by the US Treasury Department in 2024.

Doppelganger remains the most persistent Russia-based campaign, targeting many apps at once and focused primarily on weakening support for Ukraine and its government both inside the country and by the international community. It continues to add new domains to its large network of websites and attempts to promote them across the internet, while also making many errors.

[2] Adversarial Threat Report, September 2022; Recapping Our 2022 Coordinated Inauthentic Behavior Enforcements, December 2022; Q4 2022 Adversarial Threat Report, February 2023; Q2 2023 Adversarial Threat Report, August 2023; Q3 2023 Adversarial Threat Report, November 2023; Q4 2023 Adversarial Threat Report, February 2024; Q1 2024 Adversarial Threat Report, May 2024

As one of the most researched influence operations to date, Doppelganger appears to have benefited from its low quality and high discoverability in gaining notoriety and creating a perception of its omnipresence across the internet and influence far more than it has from attempting to run an actual deceptive campaign.

ADVERSARIAL ADAPTATION IN RESPONSE TO ONGOING DETECTION

Our teams are engaged in daily efforts to find and block Doppelganger's attempts to acquire new accounts and Pages, run ads, and share links to its websites and redirect domains, before these are ever shared on our apps. Here are some of our latest findings.

1. SPOOFING WEBSITES OF LEGITIMATE MEDIA EXPANDED TO LESS POLITICAL OUTLETS

With over six thousand deceptive domains operated by Doppelganger blocked on our apps, the operators continue to look for ways around detection. In the last couple of months we've seen them begin spoofing the websites of primarily non-political and entertainment news outlets and online magazines like Cosmopolitan, New Yorker, and Entertainment Weekly, in addition to health and science websites. We are adding dozens of these new spoof websites and hundreds of redirect domains to our public GitHub repository to enable broader detection and research across the internet.

2. ATTEMPTS TO SEED LINKS TO WEBSITES RESTARTED ON OUR APPS AFTER A PAUSE

At the time of our last report in May 2024, we had seen a major shift in tactics on our platform, unmatched by activity on other services. It included a pause in attempting to seed links to spoofed news and government websites on our apps, including redirects.

Since May, Doppelganger resumed its attempts at sharing links to its domains, but at a much lower rate. We blocked these latest urls from being shared on our apps. We've also seen them experiment with multiple redirect hops including TinyURL's link-shortening service to hide the final destination behind the links and deceive both Meta and our users in an attempt to avoid detection and lead people to their off-platform websites.

In typical sloppy Doppelganger fashion, the operators frequently forgot to include the actual links, even though in the text of their posts they include calls to "click on the link below."

3. CONTINUOUSLY DEGRADING AD QUALITY

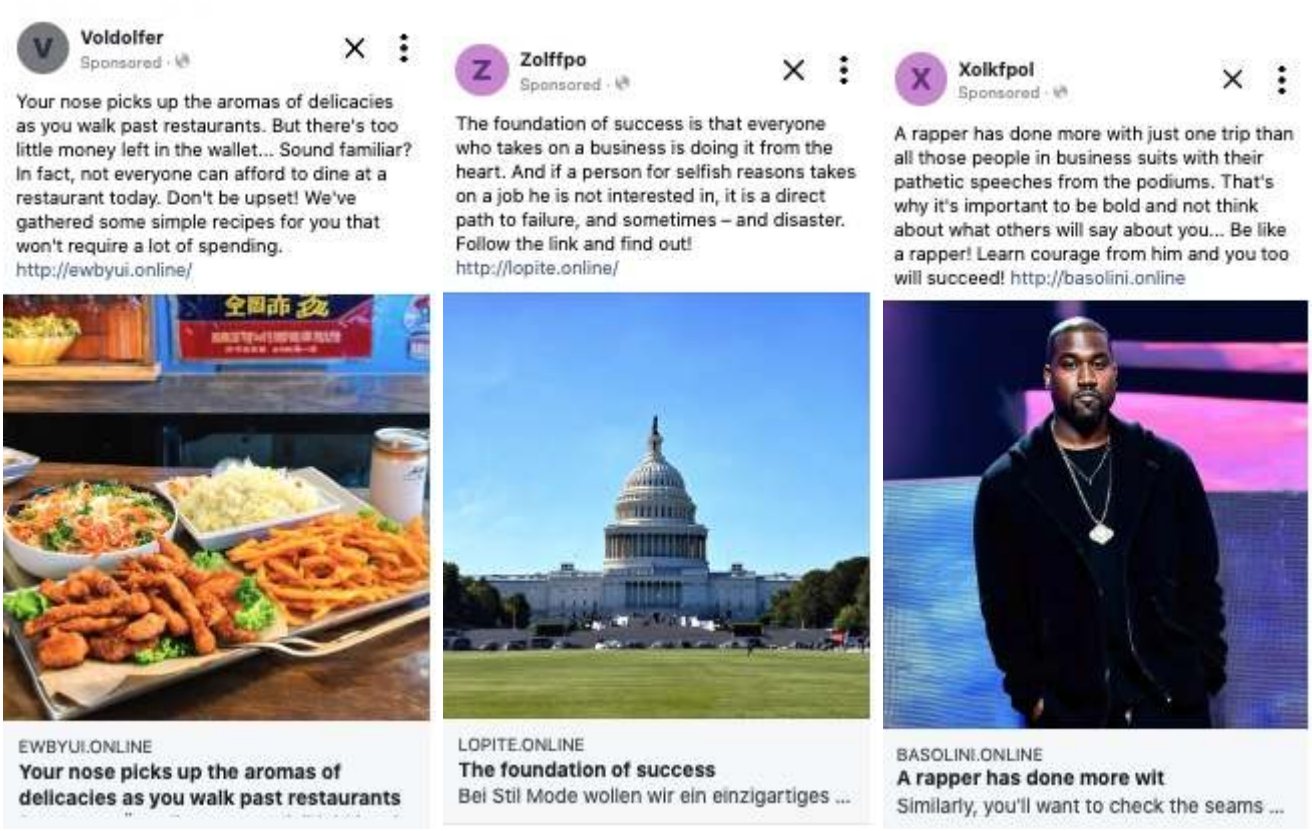
As we noted in May, Doppelganger is actively testing ways to avoid detection with the majority of ads being caught before they run or within hours after submission. We continue to incorporate our latest insights into our detection systems. These circumvention attempts are significantly

degrading the quality of these ads, making them barely legible and irrelevant to the public discourse topics this operation has been pursuing since 2022.

Here are the latest ad-related changes in response to detection:

3.1. Non-political content

In an attempt to avoid enforcement, the operators are increasingly using non-political posts and ads, focusing many of them on unrelated innocuous topics like food, health, and others. Once someone clicks on the link, they would then take people to a Russia war- or geopolitics-related article on one of the spoof domains mimicking entertainment or health publications.



Images: ads created by compromised accounts, targeting audiences in the US. They were blocked within hours.

3.2. Geofenced websites

Doppelganger continues to use geofencing to make some of its sites accessible only to internet users from particular countries. The operators use multiple random, unrelated urls to redirect people from a particular target country to geofenced spoof websites, while showing a nonsensical web page to everyone else, often making mistakes directing online users to websites in the wrong language. For example, public reporting by OpenAI cited cases when the operators “slipped up, so that some English, German and Polish articles could only be viewed from a French IP.”

Here are some examples:

Image: An ad run by a compromised Page, targeting audiences in Germany. We blocked it before it was seen by anyone.

Translation

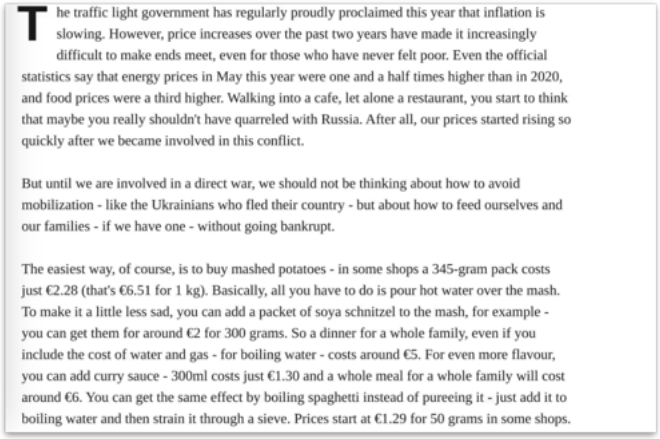
Prices are hefty in the stores but you want to eat?

We have put together a selection of recipes for dishes that you can easily prepare yourself. The groceries are inexpensive, so you can save a lot of money.

Read it yourself and tell your friends!

The ultimate destination for the link in the ad was a geofenced spoof of Cosmopolitan. A non-German online user would get directed to a web page (outside of Facebook) with nonsensical text. But a Germany-based internet user would get routed to an article on a spoofed Cosmopolitan magazine website about how the war between Ukraine and Russia leads to higher food prices and other economic issues.

Here are the screenshots of the auto-translated version of the story:


The traffic light government has regularly proudly proclaimed this year that inflation is slowing. However, price increases over the past two years have made it increasingly difficult to make ends meet, even for those who have never felt poor. Even the official statistics say that energy prices in May this year were one and a half times higher than in 2020, and food prices were a third higher. Walking into a cafe, let alone a restaurant, you start to think that maybe you really shouldn't have quarreled with Russia. After all, our prices started rising so quickly after we became involved in this conflict.

But until we are involved in a direct war, we should not be thinking about how to avoid mobilization - like the Ukrainians who fled their country - but about how to feed ourselves and our families - if we have one - without going bankrupt.

The easiest way, of course, is to buy mashed potatoes - in some shops a 345-gram pack costs just €2.28 (that's €6.51 for 1 kg). Basically, all you have to do is pour hot water over the mash. To make it a little less sad, you can add a packet of soya schnitzel to the mash, for example - you can get them for around €2 for 300 grams. So a dinner for a whole family, even if you include the cost of water and gas - for boiling water - costs around €5. For even more flavour, you can add curry sauce - 300ml costs just €1.30 and a whole meal for a whole family will cost around €6. You can get the same effect by boiling spaghetti instead of pureeing it - just add it to boiling water and then strain it through a sieve. Prices start at €1.29 for 50 grams in some shops.

Image: An ad run by a fake account, targeting audiences in France. The operation tried multiple times to run the same copy with different images of a wine glass, likely generated by AI. This ad was blocked before it was seen by anyone.

Translation

What happens if you escape from stress with a glass of wine? Nothing good, doctors tell us. And psychologists think that wine can easily be replaced by.

The ultimate destination for the link in the ad was a geofenced spoof of the online magazine Sciences Humaines. A non-French online user would get directed to a web page (outside of Facebook) with nonsensical text. But a France-based internet user would get routed to an article on a spoofed online magazine Sciences Humaines about how French citizens are drinking too much because of the stress caused by the alleged plans of President Macron to send French soldiers to Ukraine.

Image: a screenshot of a headline of the article translated to “Alcohol doesn't solve problems”

3.3. Text & image obfuscation

The operators continue to use text obfuscation tactics, including adding combinations of whitespace and extra punctuation to break up words (such as “U. kr. ai. n. e” instead of “Ukraine”). Breaking up words in these ways keeps these ads unreadable. In addition, in an apparent effort to avoid image-based detection, they attempt to use unique images for their posts. At times, they

would apply peculiar color palette edits to the same image, likely in an attempt to make them look different. This makes visuals appear defective and hard to consume.

Images: examples of ads using text and image obfuscation techniques. Four out of these five ads were blocked before anyone saw them, and one was blocked within hours after creation.

In addition, the operators used images likely generated with artificial intelligence tools in a continuous attempt to use unique visuals to avoid detection. However, these images show obvious signs of defects suggesting little quality control, if any.

These and other evasion tactics continue to result in a very poor quality of content by Doppelganger, which raises important questions about the actual intent behind these efforts, beyond just allowing the for-hire operators to check the box that the ad attempt was made. In fact, authentic users continue to comment on these ads, calling them out as Russian trolls, propaganda and bots.

4. REPURPOSING COMPROMISED PAGES & ACCOUNTS

In addition to cycling through fake accounts which get quickly detected and removed, the operators have recently expanded their use of compromised accounts and Pages, likely in an attempt to stay afloat a bit longer by appearing more authentic. At times, they would create a new Page using these accounts, and sometimes they would take over a compromised Page. These changes are quite apparent to the users who follow a Page running in one language to only discover its switch to another. We continue to detect and block these attempts by using both automation and expert investigations monitoring for these changes in tactics.

IMPACT OF PERSISTENT ENFORCEMENT

As a result of our ongoing enforcement against recidivist efforts by Doppelganger over the past two years, its operators have been forced to keep adapting and make tactical changes in an attempt to evade takedowns. These changes lead to degrading the quality of the operation's efforts, as we shared in this section. Notably, many of the adversarial shifts that appear primarily on our platforms do not show up elsewhere on the internet where the operators continue using some of their usual and known tactics (e.g., seeding direct spoof links, including article titles openly in urls, non-defective images and unobfuscated text posts, etc.). This suggests that even with the most persistent operators, persistent enforcements have significant impact on their operational capabilities. It may also be that enforcement on other platforms has driven different adaptations there. Putting together the different pieces of these campaigns across the internet can help the defender community apply a comprehensive disruption strategy against these threats.[3]

Our goal is to keep driving the operational cost of these campaigns up, making them less and less effective and we remain focused on detecting and disrupting these recidivist attempts, including by routinely sharing information about what we see.

[3] As we noted in prior reports, more research and transparency across the defender community would allow for stronger response and defenses across the internet. We shared our recommendations here and here.

08

Appendix: Threat indicators

The following section details unique threat indicators that we assess to be associated with the malicious networks we disrupted and described in this report. To help the broader research community to study and protect people across different internet services, we've collated and organized these indicators according to the Online Operations Kill Chain framework, which we use to analyze many sorts of malicious online operations, identify the earliest opportunities to disrupt them, and share information across investigative teams. The kill chain describes the sequence of steps that threat actors go through to establish a presence across the internet, disguise their operations, engage with potential audiences, and respond to takedowns.

We're sharing these threat indicators to enable further research by the open-source community into any related activity across the web (GitHub). This section includes the latest threat indicators and is not meant to provide a full cross-internet, historic view into these operations. It's important to note that, in our assessment, the mere sharing of these operations' links or engaging with them by online users would be insufficient to attribute accounts to a given campaign without corroborating evidence.

RUSSIA-BASED CIB NETWORK #1

Tactic	Threat indicator
Acquiring assets	
Acquiring Facebook accounts	76 accounts
Acquiring Facebook Pages	30 Pages
Acquiring Instagram accounts	11 accounts
Acquiring domains	https://www.yerli-media[.]org

	lurermedia[.]org
	sakartvelo-today[.]org
Acquiring YouTube channels	https://www[.]youtube.com/@Agora_Expert
Acquiring TikTok accounts	https://www[.]tiktok.com/@agora_experts_club
Disguising assets	
Posing as fictitious news outlet	yerli-media
	luremedia
	sakartvelo-today
Gathering Information	
Monitoring specific events	In Georgia, they posted about current events, including the most recent protests against the “foreign agent law.”
	In Armenia, they posted about the former Armenian official currently detained in Azerbaijan.
Targeted engagement	
Running ads	About $77,000 in spending for ads, paid for mostly in US dollars.
Engaging with users outside the operation	About 3,800 accounts followed one or more of these Pages.
	About 1,850 accounts followed one or more of these Instagram accounts.
Posting about individuals or institutions	In Georgia, they criticized protesters and supported the ruling party, Georgian Dream.
	In Azerbaijan, the operation criticized the West.
	In Armenia, they posted about politics, including supportive commentary about Russia, the former Armenian official currently detained in Azerbaijan, and criticism of the Prime Minister of Armenia.

RUSSIA-BASED CIB NETWORK #2

Tactic	Threat indicator
Acquiring assets	
Acquiring Facebook accounts	20 accounts
Acquiring Facebook Pages	14 Pages
Acquiring Instagram accounts	9 accounts
Acquiring domains to support influence operations	euronewstop[.]co[.]uk
	newstop[.]africa
Acquiring X / Twitter accounts	https://twitter[.]com/euronewstop
	https://twitter[.]com/newstop_africa
Acquiring YouTube channels	youtube[.]com/@NEWS-TOPUK
	youtube[.]com/@NEWSTOP-AFRIQUE
Acquiring Telegram channels	https[:]//t[.]me/newstopafrique
Disguising assets	
Adopting visual disguise	Fictitious journalist persona often had GAN-created (generative adversarial networks) profile pictures across the internet.
Posing as non-existent person	Fictitious journalist personas had consistent profile photos and were backstopped across several internet services.
	The Euro Top News brand purports to be a UK-based outlet with stories on international affairs under fictitious journalist bylines.
Posing as non-existent institution	EU NEWS TOP

	Newstop:Afrique
Backstopping	Fake contributors personas for fictitious news brands had presence on our platform, YouTube, Telegram, and X (formerly Twitter).
	These fictitious news brands had presence across several internet services, including ours, YouTube, Telegram, and X (formerly Twitter) to backstop these entities.
Indiscriminate engagement	
Posting on websites	The fictitious 'news' website articles often incorporated images and citations from the original sources.
Amplifying with fake accounts on social media	Fake accounts were used to post content on Facebook and drive people to the operation's off-platform assets.
Targeted engagement	
Running ads	Around $2,800 in spending for ads, paid for mostly in US dollars.
Engaging with users outside the operation	About 300 accounts followed one or more of these Pages
	about 1,800 accounts followed one or more of these Instagram accounts
Engaging with specific audience	The operation conducted French and English language campaigns.
Directing online traffic	The operation posted links to fictitious ‘news’ websites.
Posting about individuals or institutions	For the French-speaking content in Francophone Africa, the operation criticized France’s presence in the region, including through the cartoon-style images.
	For the English-speaking audiences, this campaign posted primarily about diminishing support for Ukraine in the West
	For the French-speaking content in Francophone Africa, this operation promoted Russian integration in the region.

RUSSIA-BASED CIB NETWORK #3

Tactic	Threat indicator
Acquiring assets	
Acquiring Facebook accounts	43 accounts
Acquiring Facebook Pages	85 Pages
Acquiring Telegram channels	http://t[.]me/ukreurofront
	https://t[.]me/stirid
	https://t[.]me/s/poroshenkopa
Disguising assets	
Adopting visual disguise	Fake accounts had GAN profile photos to appear unique.
Posing as non-existent person	This operation used accounts that posed as locals in the countries targeted by the operation.
Posing as non-existent institution	This operation created fictitious news outlets to 'report' on real-world stunts as if they were grassroots developments across Europe.
	This operation created a Page for a fictitious entity called the Ukrainian European Front.
Backstopping	Ukrainian European Front was backstopped on Telegram, likely to appear more legitimate to withstand scrutiny by platforms and researchers.
Evading Detection	
Obfuscating geographical location and infrastructure	This network's accounts relied on proxy IP infrastructure to hide the operators' location and were used primarily to make this campaign's Pages appear local to the countries they targeted.

Indiscriminate Engagement	
Amplifying with fake accounts on Facebook	Fake accounts were used for amplifying real-world Ukraine-related stunts in Europe, including in France, Germany, and Poland.
Targeted Engagement	
Running ads	Around $35,000 in spending for ads, paid for mostly in US dollars with the vast majority focused on Ukraine and also Moldova.
Engaging with users outside the operation	About 32,000 accounts followed one or more of these Pages, including a portion of inauthentic accounts in Brazil, which suggests attempts at purchasing fake engagement to make these Pages appear more popular than they were.
Posting about individuals or institutions	The campaign posted criticism of the current Ukraine government for failing to defend the country, low military mobilization rates and calls to hold the Presidential election in 2024 claiming that President Zelenskyy's decision to postpone it violates Article 103 of the Constitution.
	In Moldova, this campaign criticized the current government.
	In Moldova, this campaign posted about pro-Russian politicians and promoted a seemingly independent petition on the Open Petition platform calling to abolish postal voting in Moldova.

RUSSIA-BASED CIB NETWORK #4

Tactic	Threat indicator
Acquiring assets	
Acquiring Facebook accounts	12 accounts
Acquiring Facebook Pages	32 Pages
Acquiring Facebook Groups	5 Groups

Acquiring Instagram accounts	3 accounts
Disguising assets	
Adopting visual disguise	Some of the accounts used profile photos likely created using Generative Adversarial Networks (GAN).
Posing as non-existent institution	The people behind this operation managed Pages posing as Ukrainian organizations.
Impersonating real person	The people behind this operation impersonated public figures in the West including some pro-Russia commentators.
Evading Detection	
Copying authentic content	This cluster posted content copied from public figures in the West including some pro-Russia commentators that this operation tried to impersonate.
Obfuscating infrastructure	This operation used proxy IP addresses to appear to be based in the regions it targeted.
Targeted Engagement	
Running ads	Around $41,000 in spending for ads, paid for mostly in Sri Lankan rupees and US dollars.
Engaging with users outside the operation	About 23,000 accounts followed one or more of these Pages.
	About 280 accounts followed one or more of these Instagram accounts.
	Around 18,500 accounts joined one or more of these Groups.
Posting about individuals or institutions	The Ukraine cluster posted about domestic politics, conscription, claims of disinformation, and criticism of the government and President Zelenskyy.
	In Polish, this network posted about Ukrainian migrants, including suggesting that Polish schools should teach students Ukrainian language, history and literature to help Ukrainian refugees to feel more comfortable in Poland.
	The efforts targeted at the EU and US focused primarily on posting about Western aid provided to Ukraine, war casualties among Ukrainian soldiers, claims that Ukraine's government has failed to protect its people, and criticism of the West for providing lethal weapons to Ukraine and for allowing war crimes in Gaza.

VIETNAM-BASED CIB NETWORK

Tactic	Threat indicator
Acquiring assets	
Acquiring Facebook accounts	112 accounts
Acquiring Facebook Pages	65 Pages
Acquiring Instagram accounts	49 accounts
Acquiring X / Twitter accounts	https://twitter[.]com/ShameOnQatar24
	https://twitter[.]com/ItsIn_YourHands
	https://twitter[.]com/Shi3aDodelharb
	https://twitter[.]com/lallihtilalalir
	http://x[.]com/shi3adodelharb
	http://x[.]com/1701now
Acquiring YouTube channels	https://www[.]youtube.com/@ItsInYourHands
	https://www[.]youtube.com/@Shi3aDodelharb
	https://www[.]youtube.com/@KowtnabeWe7dtna
Acquiring TikTok accounts	https://www.tiktok[.]com/@shi3adodelharb
Acquiring Telegram channels	http://t[.]me/kowatnabewe7detna
	https://t[.]me/DohaDirt
	https://t[.]me/MadeInQatar24
Acquiring other accounts	https://www.pinterest[.]com/shi3adodelharb/
Creating online petitions	https://www[.]change.org/p/1701-the-hope-of-lebanon-%D9%A1%D9%A7%D9%A0%D9%A1-%D8%A7%D9%85%D9%84-%D9%84%D8%A8%D9%86%D8%A7%D9%86

Acquiring domains	itsinyourhands24[.]com
	shameonqatar[.]com
	shi3adodelharb[.]com/
	kowatnabewe7detna[.]com
	1701now[.]com
Disguising assets	
Adopting visual disguise	The network used fake accounts with GAN profile photos – the majority of which were detected by our automated systems prior to this investigation – to run ads and manage Pages.
	The Lebanon-targeting campaign had consistent visual branding across several platforms on the internet.
Posing as non-existent institution	It's in Your Hands, claimed to be "an informal coalition of Christian leaders and organizations around the world working on helping the hostage families since October."
Backstopping	Several of the regional campaigns established and maintained a presence across various platforms and websites.
Targeted engagement	
Running ads	Around $1.2 million in spending for ads, paid for mostly in Vietnamese dongs.
Engaging with users outside the operation	About 38,000 accounts followed one or more of these Pages.
	0 accounts followed these Instagram accounts.
Engaging with specific audience	The operation conducted multiple language-specific campaigns.
	The French- and Arabic-language campaign efforts targeted Lebanon. It posted criticism of Iran's involvement in the Israel-Hamas war, and called for Lebanon to avoid the repeat of the 2006 war in the region.
	The French-language efforts included posting criticisms of Shia Islam and Qatari investments in Europe.
	The French- and Arabic-language campaign efforts targeted Lebanon and posted in support of Palestine.
	The French-language effort targeted France and posted about the importance of retaining traditional French values and secularism

Co-opting real people / organizations	The individuals behind this activity appeared to have engaged an American celebrity to record a video plea to Sheikha Moza bin Nasser, the mother of the Emir of Qatar.
Directing online traffic	The operation directed traffic to the campaign websites and its off-platform accounts.

US-BASED CIB NETWORK

Tactic	Threat indicator
Acquiring assets	
Acquiring Facebook accounts	96 accounts
Acquiring Facebook Pages	16 Pages
Acquiring Facebook Groups	12 Groups
Acquiring Instagram accounts	3 accounts
Acquiring domains	patriotsrunproject[.]com
	patriotsrunmn[.]com
	patriotsrunnv[.]com
	patriotsrunoh[.]com
	patriotsrunmt[.]com
	patriotsrunaz[.]com
	patriotsrunmi[.]com
	patriotsrunwi[.]com
	patriotsrunpa[.]com
	patriotsrunnc[.]com
Acquiring X / Twitter accounts	https://x[.]com/PRPNational

Disguising assets	
Adopting visual disguise	This operations ran accounts appeared to have been acquired from Bangladesh, with many starting out with GAN profile photos and later changing to other images
Posing as non-existent person	Their fictitious personas pretended to be living in states like Arizona, Michigan, Nevada, Ohio, Pennsylvania, Wisconsin, and North Carolina. To seem more credible, they often interspersed the PRP-related posts with local content related to state sports teams and events, and local restaurant check-ins, in addition to political memes which they copied from other people on the internet.
Posing as non-existent institution	This campaign centered around a fictitious political advocacy group – the Patriots Run Project or PRP.
Backstopping fictitious individual across multiple websites	This operation included websites and social media accounts, including on our apps and X (formerly Twitter).
Gathering Information	
Monitoring specific events	The network posted about US elections and primaries.
Evading Detection	
Copying authentic content	The fake accounts copied political memes from other people on the internet.
Obfuscating location & infrastructure	This operation's fictitious personas maintained relative operational security (OpSec) by using proxies to pretend to be living in the particular states this campaign targeted.
Indiscriminate Engagement	
Amplifying with fake accounts on Facebook	Fake accounts were used to amplify PRP's content to make it appear more popular than it was.
Posting on websites	This operation included websites that represented the state chapters of PRP in states like Arizona, Michigan, Nevada, Ohio, Pennsylvania, Wisconsin, and North Carolina.
Targeted engagement	
Running ads	Around $50,000 in spending for ads, paid for mostly in US dollars.
Engaging with users outside the	About 1,700 accounts followed one or more of these Pages.

operation	About 2,300 accounts followed one or more of these Instagram accounts. Around 1,200 accounts joined one or more of these Groups.
Posting about individuals or institutions	The network posted about US elections and primaries, including criticisms of “Republican and Democrat elites”, “God”, “guns”, and “illegal immigrants.”

LATEST THREAT INDICATORS RELATED TO RECIDIVIST ATTEMPTS

We monitor for, and enforce against, efforts to come back by networks we previously removed. Some of these networks attempt to create new off-platform entities, such as websites or social media accounts, as part of their recidivist activity.

We’re sharing some of these novel threat indicators related to recidivism attempts to enable further research by the open-source community into any related activity across the internet. It’s important to note that, in our assessment, the mere sharing by online users of these operations’ links or engaging with them would be insufficient to attribute these accounts to a given campaign without corroborating evidence.

DOPPELGANGER UPDATE: LATEST SPOOFED DOMAINS

This section includes the latest domains (as of July 31, 2024) that are spoofing news, entertainment and other websites which we’ve identified as part of the Doppelganger campaign.

In addition to these domains, we’ve identified hundreds more that the campaign uses to redirect people to its spoofing websites. We’ve updated our full list of threat indicators linked to Doppelganger on GitHub in a machine-readable format.

Domains spoofing news sites

Domain	Registration date	Country likely targeted
closermag[.]eu	10 July 2024	France
conspiracywatch[.]in	15 July 2024	France
historia[.]fyi	4 July 2024	France
lefigaro[.]foo	7 July 2024	France
leparisien[.]wf	18 May 2024	France
psychologies[.]top	21 June 2024	France
scienceshumaines[.]sbs	25 June 2024	France
thuriesmagazine[.]in	5 July 2024	France

berliner-zeitung[.]in	21 July 2024	Germany
bibelbund[.]cfd	7 July 2024	Germany
geo[.]frl	17 July 2024	Germany
herder[.]in	7 July 2024	Germany
onmeda[.]click	17 July 2024	Germany
psychologie-heute[.]eu	10 July 2024	Germany
spektrum[.]cfd	25 June 2024	Germany
zeit[.]cx	5 July 2024	Germany
israeltoday[.]top	4 July 2024	Israel
lilith[.]day	3 July 2024	Israel
ciekawostkihistoryczne[.]in	7 July 2024	Poland
dzieckowpodrozy[.]in	7 July 2024	Poland
dzienniknaukowy[.]link	3 July 2024	Poland
mynaszlaku[.]in	15 July 2024	Poland
polityka[.]link	6 April 2024	Poland
polskieradio[.]cfd	16 June 2024	Poland
beautynewsnyc[.]cfd	7 July 2024	United States
cosmopolitan[.]day	4 July 2024	United States/Germany
eatingwell[.]cfd	17 July 2024	United States
ew[.]pe	n/a	United States
forward[.]pw	16 June 2024	United States
graziamagazine[.]cfd	9 July 2024	United States
medicalhomeportal[.]boo	15 July 2024	United States
mensjournal[.]day	7 July 2024	United States
newyorker[.]bz	10 May 2024	United States
oah[.]icu	17 July 2024	United States
realsimple[.]sbs	17 June 2024	United States
slate[.]bz	25 June 2024	United States
wanttoknow[.]in	5 July 2024	United States