DECEMBER 2024

THIRD QUARTER

Adversarial Threat Report

Margarita Franklin, Director, Public Affairs, Security
Mike Torrey, Security Engineer

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 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

In this report, we're sharing threat research into five covert influence operations we disrupted, including from India, Iran, Lebanon and Moldova (first reported on October 11, 2024). We detected and removed these campaigns before they were able to build authentic audiences on our apps. We're also including an update on the most persistent Russian covert influence operation known as Doppelganger.

In addition, as we look back to 2024, here are some key insights into the global threat landscape (for our broader integrity insights see here):

Global enforcements: 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 31 CIB networks, and China, with 11. This year, our teams have taken down around 20 new covert influence operations around the world, including in the Middle East, Asia, Europe and the US.

Use of GenAI by CIB networks: Throughout the year, we've continued to watch for and assess the risks associated with evolving new technologies like AI. Our findings so far suggest that GenAI-powered tactics have provided only incremental productivity and content-generation gains to the threat actors, and have not impeded our ability to disrupt their covert influence operations. Our existing defenses in countering adversarial threat activity, including our focus on behavior, rather than content (whether it's generated with AI or not), apply and appear effective at this time. However, we remain vigilant and continue to monitor as malicious tactics evolve. Here are some examples of the use of GenAI by CIB networks we've disrupted in Q3'2024:[1]

- Fake accounts using profile photos created using generative adversarial networks (GAN);
- Fictitious news brands posting AI-generated video newsreaders across the internet.

Struggling to build authentic audiences: The majority of the CIB networks we've disrupted this year have struggled to build authentic audiences, and some used fake likes and followers to appear more popular. For example, we took down a CIB network originating primarily in the Transnistria region of Moldova, and targeted Russian-speaking audiences in Moldova. The vast majority of its followers were outside of Moldova, which suggests the use of inauthentic engagement tactics to make these efforts appear more popular than they actually were.

Cross-internet nature of CIB campaigns: The vast majority of the CIB networks we disrupted globally tried to spread themselves across many online apps, including ours, YouTube, TikTok, X, Telegram, Reddit, Medium, Pinterest, and more. We've seen a number of influence operations shift much of their activities to platforms with fewer safeguards. For example, fictitious videos about the US elections – which were assessed by the US intelligence community to be linked to Russian-based influence actors – were seeded on X and Telegram. In a minimal number of instances

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

where people in the US reposted this content on our platform, we labeled the content as reported to be linked to Russian influence operations.

Running websites to withstand takedowns by social media: Most of the CIB networks we've disrupted this year ran their own websites, likely to withstand takedowns by any one company. The largest and most persistent such operation known as Doppelganger continues to use a vast web of fake websites, including some spoofing legitimate news and government entities. We have created the largest repository of Doppelganger's threat indicators exposing over 6,000 domains since 2022 for researchers and other investigative teams to see so they can take appropriate action, in addition to blocking these malicious domains from being shared on our apps. However, despite some welcome disruptions by governments and others, many of Doppelganger's web domains we have exposed to date have been quickly replaced and continue to post new content, and many of their brands remain active on X and Telegram.

Doppelganger & US elections: Ahead of the US election, Doppelganger struggled to get through on our apps and largely abandoned posting links to its websites. We stopped the vast majority of Doppleganger's attempts to target the US in October and November before any user saw them.

Persistent tactical adaptations lead to strategic failures: As a result of our ongoing aggressive enforcement against recidivist efforts by Doppelganger, its operators have been forced to keep adapting and make tactical changes in an attempt to evade takedowns. These changes have led to degrading the quality of the operation's efforts, rendering these attempts impossible to comprehend by an average online user. In addition, 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 older known tactics. This suggests agility in response to detection by various services and we expect to see more changes over time.

01

Moldova

****Originally reported on October 11, 2024*

We removed seven Facebook accounts, 23 Pages, one Group and 20 accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated primarily in the Transnistria region of Moldova, and targeted Russian-speaking audiences in Moldova. We removed this campaign before they were able to build authentic audiences on our apps.

This operation centered around about a dozen fictitious, Russian-language news brands posing as independent entities with presence on multiple internet services, including ours, Telegram, OK (Odnoklassniki), and TikTok. It included brands like Tresh Kich, Moldovan Mole, Insider Moldova, Gagauzia on Air.

The individuals behind this activity used fake accounts – some of which were detected and disabled prior to our investigation – to manage Pages posing as independent news entities, post content, and to drive people to this operation's off-platform channels, primarily on Telegram. Some of these accounts went through significant name changes over time and used profile photos likely created using generative adversarial networks (GAN).

They posted original content, including cartoons, about news and geopolitical events concerning Moldova. It included criticism of President Sandu, pro-EU politicians, and close ties between Moldova and Romania. They also posted supportive commentary about pro-Russia parties in Moldova, including a small fraction referencing exiled oligarch Shor and his party. The operators also posted about offering money and giveaways, including food and concert tickets, if people in Moldova would follow them on social media or make graffiti with the campaign's brand names.

This campaign frequently posted summaries of articles from a legitimate news site point[.]md, but with an apparent pro-Russia and anti-EU slant added by the operators. They also amplified a Telegram channel of the host of a satirical political show in Moldova critical of pro-European candidates. One of this operation's branded Telegram channels was promoted by a Page we removed last quarter as part of a Russia-origin CIB network (case #3 in the Q2 2024 report).

We found this network as part of our internal investigation into suspected coordinated inauthentic behavior in the region. Although the people behind this activity attempted to conceal their identity and coordination, our investigation found links to individuals from Russia and Moldova operating from the Transnistria region, including those behind a fake engagement service offering fake likes and followers on Facebook, Instagram, YouTube, OK, VKontakte, X and the petition platform

Change.org. We also found some limited links between this CIB activity and a network from the Luhansk region in Ukraine that we removed in December 2020.

- *Presence on Facebook and Instagram:* 7 Facebook accounts, 23 Pages, 1 Group and 20 Instagram accounts.
- *Followers*: About 4,200 accounts followed one or more of these Pages, no accounts joined this Group, and around 335,000 accounts followed one or more of these Instagram accounts. The vast majority of these followers were outside of Moldova, which suggests the use of inauthentic engagement tactics to make these efforts appear more popular than they actually were.
- *Ad spend:* About $4,000 in spending for ads, paid for mostly in US dollars.

02

India

We removed 122 accounts on Facebook, two Pages, and 30 accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in India and targeted domestic audiences in that country across multiple internet services including ours, YouTube, and X (formerly Twitter).

The people behind this activity used fake accounts – some of which were detected and disabled by our automated systems prior to our investigation – to manage elaborate fictitious personas, post content and manage Pages. These accounts had a corresponding presence on YouTube and X to backstop the operation's fake personas so they appear more legitimate and can withstand scrutiny by platforms and researchers. This network showed relatively consistent operational security (OpSec) aimed to conceal its deceptive activity.

While this campaign created original content, it also amplified posts by official political accounts in an attempt to make them appear more popular than they were. The people behind this effort posted primarily in English and Hindi about news and current events in India, including elections and political parties, and India's economic development.

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

- *Presence on Facebook and Instagram:* 122 Facebook accounts, two Pages, and 30 accounts on Instagram.
- *Followers:* About 136,000 accounts followed one or more of these Pages, and about 1,100 accounts followed one or more of these Instagram accounts.
- Ad spend: About $9,900 in spending for ads, paid for mostly in Indian rupees.

03

India

We removed 100 Facebook accounts, two Pages, and 19 accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in the Odisha region of India and targeted people in that region.

The individuals behind this activity used fake accounts – some of which were detected and disabled by our automated systems prior to our investigation – to post, comment, and amplify other people's content. Many of these accounts have gone through significant name changes over time. They also created fictitious personas posing as locals and purporting to post about family events, hobbies, food, and other activities, likely to appear more authentic so they can withstand scrutiny by platforms and researchers. These personas attempted to befriend people in the Odisha region and restricted their own accounts' visibility to 'friends only,' in an apparent attempt to control their discoverability.

The network posted primarily in English and Hindi about news and current events in India, including elections and local candidates from a regional party in India.

We found this activity as a result of our internal investigation into suspected coordinated inauthentic behavior in the region. We removed this network before it was able to build an audience among authentic communities.

- *Presence on Facebook and Instagram:* 100 Facebook accounts, 2 Pages, and 19 Instagram accounts.
- *Followers:* About 4,600 accounts followed one or more of these Pages and about 150 accounts followed one or more of these Instagram accounts.
- *Ads*: Around $20 in spending for ads, paid for mostly in Indian rupees.

04

Iran

We removed 48 Facebook accounts and two accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in Iran and targeted primarily Israel. We removed it before it was able to gain traction among authentic audiences on our apps.

The operation ran five fictitious brands – Zeus, Cyber Court, Net Hunter, Regiment Groupe Union Defense (RGUD), and WeRedEvils0g – posing as anti-West activist or hacktivist collectives. They had unique visual branding, slogans and presence across the internet, including on our apps, YouTube, Telegram, X, and their own websites.

One brand called for banning Israeli athletes from participating in the Paris Olympics, attracting the attention of French authorities. Two others appeared to have appropriated the branding of previously existing entities but with slight modifications. One of these brands also ran a website mimicking the Jerusalem Post where they published their content.

On our apps, the individuals behind this campaign used fake accounts – some of which were detected and disabled by our automated systems – to post, comment, reshare, and drive people to off-platform sites where they claimed to host hacked documents from Israeli government agencies. We are unable to assess the validity of these claims. Many of these accounts were created only days before posting. Some of their comments were made under unrelated posts by authentic users from years ago. The operators posted infographics, videos, and other content in English, Hebrew and French, while using proxy IP infrastructure to conceal their origin. To evade detection, this campaign used link shorteners which first led to Tor onion sites only accessible via Tor browser. The only content on these Tor pages was links to newly-created Telegram channels.

We found this network as a result of our internal investigation and linked it to an Iranian threat actor, Cotton Sandstorm, which Microsoft previously connected to Iran's Islamic Revolutionary Guard Corps or IRGC. We also found some connections to the CIB network we reported on in May 2023. As we were preparing this report, the FBI, US Department of Treasury, and Israel National Cyber Directorate published a joint advisory linking most of the brands run by this operation to the Iranian cyber group Emennet Pasargad.

- *Presence on Facebook and Instagram:* 48 Facebook accounts and 2 Instagram accounts.
- *Followers:* About 10 accounts followed one or more of these Instagram accounts.

05

Lebanon

We removed 15 Facebook accounts, 15 Pages, and 6 accounts on Instagram for violating our policy against coordinated inauthentic behavior. This network originated in Lebanon and targeted primarily Israel. We removed it before it was able to build authentic audiences on our apps.

This operation centered around three fictitious news entities called Dofek, Israel in a Minute, and Halalom Israel. Each of them had distinct branding and presence across multiple platforms, including ours, YouTube, X, TikTok, in addition to their own websites where they shared both socio-political and non-political content about football, technology and other topics.

The people behind this activity used fake accounts – many of which were detected and disabled by our automated systems prior to this investigation – to manage branded Pages posing as independent news entities and to post content. Some of these accounts used profile photos likely generated using artificial intelligence such as Generative Adversarial Networks (GAN), including one fictitious journalist persona. The operators used proxy IP infrastructure to conceal where this activity is coming from. One of the brands – Israel in a Minute – frequently posted AI-generated video newsreaders across the internet.

This network posted original content in Hebrew about news and geopolitical events in Israel with generic hashtags like #Israel, #Jerusalem, #Netanyahu, among others. It included posts about Israel's dependence on US support, claims that Israeli people are leaving the country, claims of food shortages in Israel, and criticism of the Israeli government and its military strikes in the Middle East.

We began looking into this operation after reviewing information about a portion of its activity shared by the open-source research community. Although the people behind this operation attempted to conceal their identity and coordination, our investigation found links to individuals in Lebanon, including some with links to two media entities: Al Mayadeen in Lebanon and LuaLua TV registered in the UK.

- Presence on Facebook and Instagram: 15 Facebook accounts, 15 Pages and 6 Instagram accounts.
- Followers: About 5,000 accounts followed one or more of these Pages and about 5,200 accounts followed one or more of these Instagram accounts.
- Ads: Around $9,000 in spending for ads on Facebook and Instagram, paid for mostly in US dollars.

06

Russia

DOPPELGANGER'S ATTEMPTS TO STAY AFLOAT ACROSS THE INTERNET

As part of our ongoing reporting on Doppelganger, a cross-internet influence operation from Russia, we're sharing our **9th** update in **26** months that includes our latest research into this malicious activity.[2] It includes new attribution insights and notable shifts in tactics in response to our ongoing aggressive enforcement. We're also adding about **600** new threat indicators to our industry's largest repository of **6,000+** signals related to this campaign so that our peers and researchers can investigate and take action as appropriate.

WHAT IS DOPPELGANGER?

In 2022, we were the first technology company to publicly report on Doppelganger, an operation centered around a network of websites spoofing legitimate news outlets. The EU Disinfo Lab and the Digital Forensic Research Lab published their research at the same time.

Attribution: Doppelganger appears to be the work of multiple groups of operators. In December 2022, we were the first to publicly attribute it to two companies in Russia – Structura National Technology and Social Design Agency. They were sanctioned by the EU in 2023 and by the US Treasury Department in 2024, with the US and French governments adding new elements to the attribution. **We can now share that our latest investigation also found links between some of Doppelganger's activities and individuals associated with MGIMO (Moscow State Institute of International Relations).**

Doppelganger remains the most persistent Russia-based campaign targeting many apps at once and focused primarily on weakening support for Ukraine both inside the country and by the international community. It continues to add new domains to its vast network of websites and attempts to promote them across the internet, typically failing to build engagement among authentic audiences and exaggerating its own success.

[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, Q2 2024 Adversarial Threat Report, August 2024

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 accounts on other online services and websites. Here are some of our latest findings:

No more 'doppel' in 'Doppelganger' on our apps

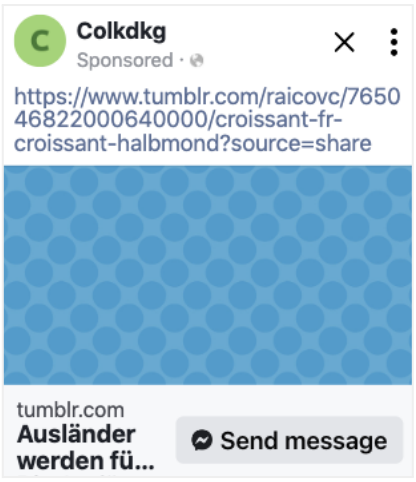
Likely in response to our ongoing blocking of its domains, we no longer see Doppelganger attempting to direct people on our apps to its domains mimicking websites of news outlets or government entities. However, we keep monitoring for changes in this behavior as we continue to see them seeding these domains elsewhere online.

Persistent website infrastructure enabled by fractured domain name ecosystem

Doppelganger continues to put extensive efforts into operating its websites, likely to preserve its content against ongoing and repeat takedowns by social media apps. In recent months, we've seen some welcome disruptions and seizures of this campaign's web infrastructure by government and other entities, including some of the domains we had exposed publicly. However, the operators quickly replaced many of these websites by moving them to new hosting providers and top-level domains (sometimes in less than 24 hours) where they continue to post new content to this day.

Hosting content on Reddit, Pinterest, Tumblr, and Medium

Between mid-October and mid-November, Doppelganger hosted text and image content on internet services like Reddit, Pinterest, Tumblr, and Medium. The operators then tried to post links to this off-platform content on our apps, likely in an attempt to circumvent our automated detection. As usual, we share our findings with our peers when possible and have seen some of these assets come down. Here are some examples:



Images
Examples of attempted ads containing links to off-platform hosted content only. They were blocked and never ran.

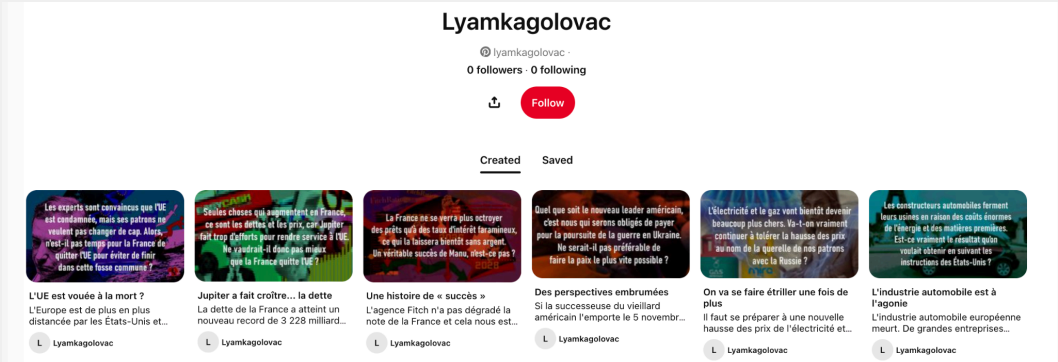


Image: Example of Doppelganger staging and hosting content on Pinterest which they later attempted to promote on Facebook. The ads were blocked and never ran.

Using GenAI to create unique images

The operators used unique, non-political images likely generated with artificial intelligence tools in a continuous attempt to evade automated image detection. However, these images show obvious signs of defects suggesting little quality control, if any. They included images of hands with 6 or more fingers, objects melting into one another, a picture of a flaming burger with a disembodied hand on fire behind it.

Text & image obfuscation tactics

Doppelganger continues to use text obfuscation tactics in an attempt to avoid automated key word detection. Recently, we've seen the operators adding periods, spaces and dashes (such as "le. ad. Er" instead of leader or "so. ldi-er" instead of soldier), rendering their content effectively unreadable. They also experimented with not using politicians' names, replacing them with nicknames which appear odd and irrelevant for native speakers.

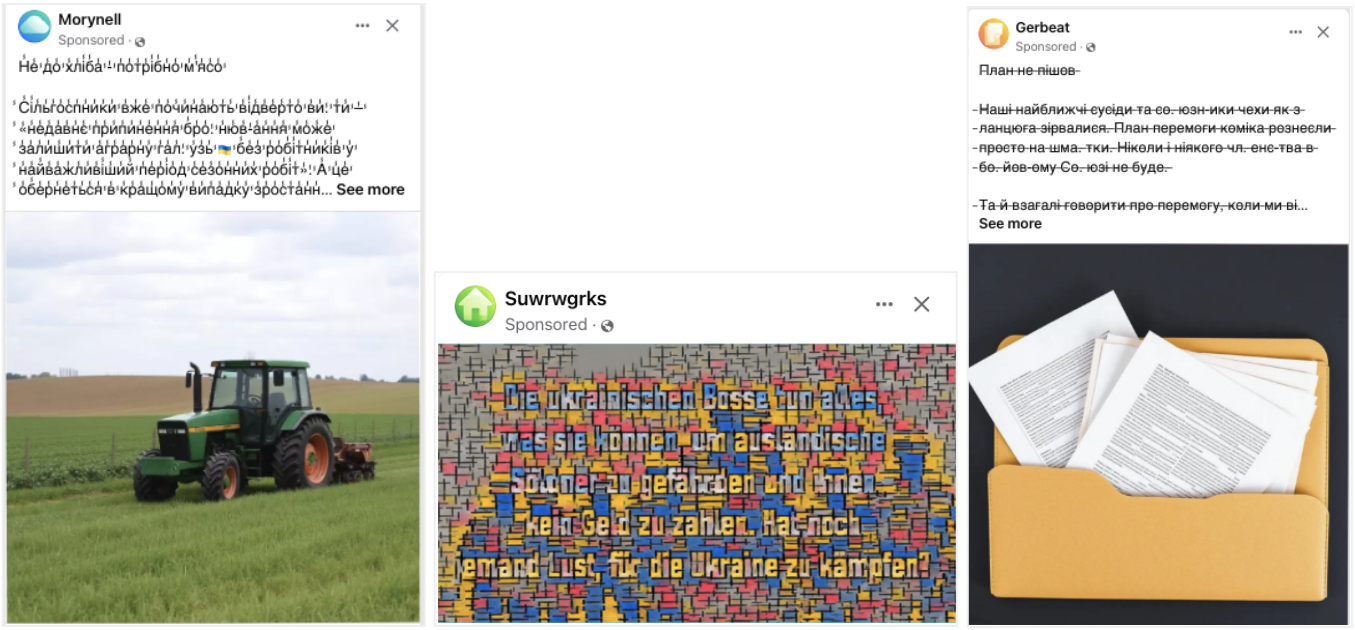


Image: Examples of Doppelganger's obfuscation tactics. These ads were blocked and never ran.

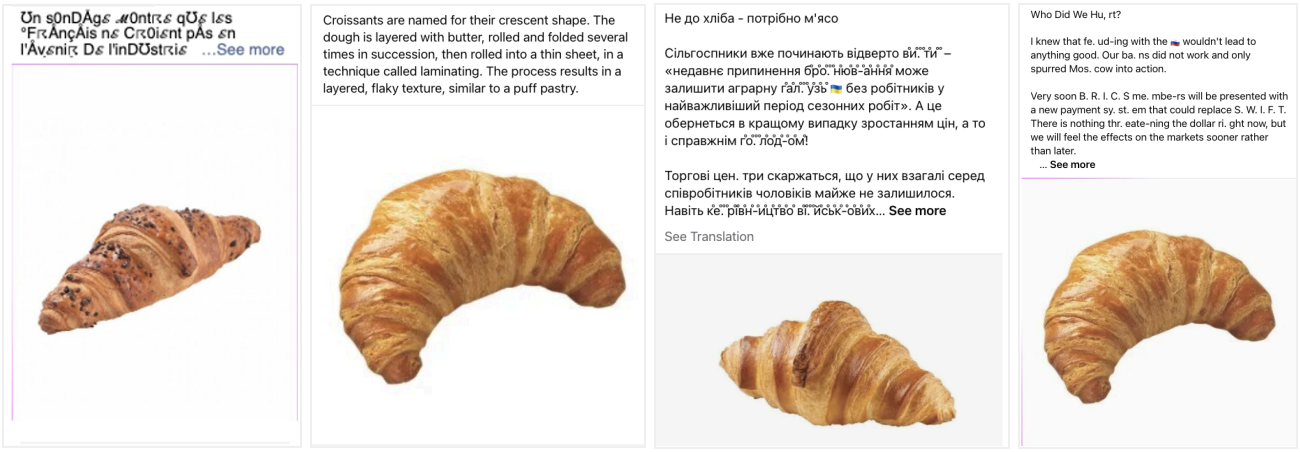
Likely to probe our automated detection, after a failed attempt at submitting an ad, the operators iterated with many more versions of the same ad as they made it less and less legible. They tried moving letters out of order and increasing the width of the strikethrough line until it completely covered up the text in the image so it was no longer visible.

Images:

Above: The original image we blocked

On the right: Examples of further attempts to obfuscate image and text rendering them unreadable. They were also blocked.

In peculiar croissant-obsessed attempts to iterate and probe our ad defenses, we saw Doppelganger's operators spend time just before the US elections by repeatedly trying to submit ads that either included a photo of a croissant, or text about a croissant, or a photo of a croissant alongside politics-related text, or a political photo alongside a croissant-related text, or a non-croissant post containing a link with a word croissant in it. We saw similar croissant content posted by Doppelganger on other internet services. We blocked these ads on our apps from running before anyone saw them. Here are some examples:



LOOKING AHEAD

No signs of slowing down, even in the face of being ineffective

While persistence is common among influence operations, Doppelganger has taken it to a new level over the last 2.5 years, while remaining crude and largely ineffective in building authentic audiences on social media. We expect this campaign run by for-hire operators at the direction of the Russian Presidential Administration in wartime to keep at it for as long as their clients' operational objectives remain.

Persistent tactical adaptations lead to strategic failures

As a result of our ongoing enforcement against recidivist efforts by Doppelganger, its operators have been forced to keep adapting and make tactical changes in an attempt to evade takedowns. These changes have led to degrading the quality of the operation's efforts, as the examples we shared show, rendering these attempts impossible to comprehend by an average online user. In addition, 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 older known tactics (e.g., seeding direct spoof links, non-defective images and unobfuscated text posts, etc.). This suggests agility in response to detection by various services and we expect to see more changes over time.

'Election targeting' just a means to an end

In the last 2.5 years, Doppelganger has veered into domestic politics in various countries, including ahead of the US elections. However, these efforts were consistently in the context of undermining the international community's support for Ukraine when the ongoing war became part of the election discourse in a particular country. We expect the operators to continue these efforts, including in the context of 2025 elections globally. As we have already observed, this could take the shape of blaming economic hardships in specific countries 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.

Persistence in offense requires persistence in defense

We have seen that operations like Doppelganger – no matter how ineffective – don't just stop in response to a single takedown by one platform or a one-time domain seizure. These are well-resourced, for-hire campaigns tasked by their clients to keep going. However, we have also seen how relentless repeat takedowns on our apps over long periods of time can lead to diminishing results and increased frictions for the operators who continue to waste their time and resources in trying to probe and evade detection. Moving forward, we can collectively raise our cross-industry defenses with a stronger concerted effort to share information and disrupt the internet infrastructure powering these campaigns. Otherwise, these website-centric efforts will persist by exploiting the fractured enforcement landscape, including the domain name ecosystem.

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.

MOLDOVA-BASED CIB NETWORK

Tactic	Threat indicator
Acquiring Assets	
Acquiring Facebook accounts	7 accounts
Acquiring Facebook Pages	23 Pages
Acquiring Facebook Groups	1 Groups
Acquiring Instagram accounts	20 accounts
Acquiring TikTok accounts	tiktok[.]com/@trech_kich6
	tiktok[.]com/@kishinev24

	tiktok[.]com/@moldova_acum
Acquiring Telegram channels	t[.]me/**insider_md**
	t[.]me/**trech_kich**
	t[.]me/**onlinemd24**
	t[.]me/**md_krot**
	t[.]me/fluieras
	t[.]me/kishinev24
	t[.]me/chsreal
	t[.]me/moldova_acum
	t[.]me/gagauzia_v_efire
	t[.]me/beltsy24
	t[.]me/trech_kich_chat
	t[.]me/trech_kich_bot
Acquiring other social media assets	ok[.]ru/group/70000005349948
Disguising Assets	
Creating fictitious news outlets	Insider Moldova
	Треш Киш - Trech Kich
	Молдова онлайн - Moldova Online

	Молдавский Крот - Moldovan Mole
	Флуераш - Fluieras
	Кишинев - Kishinev
	Реальный Кишинев - Real Chisinau
	Молдова сейчас - Moldova Acum
	Гагаузия в эфире - Gagauzia on Air
	Бельцы 24 - Beltsy 24
Adopting visual disguise	Using profile photos likely generated using artificial intelligence such as Generative Adversarial Networks (GAN)
Evading Detection	
Camouflaging content	Frequently posting summaries of articles from a legitimate news site point[.]md, but with an apparent pro-Russia and anti-EU slant added by the operators
Targeted Engagement	
Running Ads	About $4,000 in spending for ads on Facebook, paid for mostly in US Dollars
Engaging with users outside the operation	About 4,200 accounts followed one or more of these Pages
	About 335,000 accounts followed one or more of these Instagram accounts. The vast majority of these followers were outside of Moldova, which suggests the use of inauthentic engagement tactics to make these efforts appear more popular than they were.
Engaging with specific audience	Targeting Russian-speaking audiences in Moldova

Directing online traffic	Using fake accounts to drive people to this operation's off-platform channels, including Telegram channels
Posting about individuals or institutions	Posting original content that included criticism of President Sandu, pro-EU politicians, and close ties between Moldova and Romania.
	Posting supportive commentary about pro-Russia parties in Moldova, including a small fraction referencing exiled oligarch Shor and his party

IRAN-BASED-CIB NETWORK

Tactic	Threat indicator
Acquiring assets	
Acquiring Facebook accounts	48 accounts
Acquiring Instagram accounts	2 accounts
Acquiring domains	CyberCourt[.]io
	jerusalem-news[.]com
	rgud-group[.]com
	zeusistalking[.]net
	zeusistalking[.]com
	rgud-group[.]net
Acquiring X / Twitter accounts	x[.]com/zeus_is_talking

	x[.]com/rgud181178
Acquiring Telegram channels	t[.]me/weredevils0g
	t[.]me/zeus_is_talking
	t[.]me/cybercourt_io
	t[.]me/zeus_leak
	t[.]me/Nethunt3r
	t[.]me/makhlab_al_nasr
	t[.]me/anonymous_south_africa
	t[.]me/zeus_leak2
	t[.]me/ze_us_is_talking4
	t[.]me/ze_us_is_talking5
	t[.]me/rgud_chanel
	t[.]/RGUD_bot
Disguising Assets	
Impersonating news website	The operation impersonated a real news website under the alias jerusalem-news
Impersonating real institution	Two of these campaign brands appeared to have appropriated branding of existing groups with slight modifications – a Paris-based anti-Zionist entity and an Israel-based hacker collective.
Indiscriminate Engagement	

Amplifying with likely fake accounts on social media	The fake accounts were used to amplify the main operation campaign brands including in comments to other people's posts
Targeted engagement	
Directing online traffic	The individuals behind this campaign used fake accounts to drive people to off-platform websites where they claimed to be hosting allegedly hacked documents
	They also used on-platform accounts to seed links to their off-platform channels on Telegram
Posting about individuals or institutions	the 'Zeus' campaign posted allegedly hacked material about Israeli olympic athletes during the Paris Olympics
Offering or posting allegedly hacked material about individuals or institutions	xss[.]is/members/363554
	leakbase[.]io/nethunt3r
	altenes[.]is/members/nethun3r.141588
	www.nulled[.]to/user/60944541-nethunt3r
	cracked[.]io/NetHunt3r
	craxpro[.]io/nethunt3r
	CyberCourt[.]io
	jerusalem-news[.]com
	rgud-group[.]com
	zeusistalking[.]net
	zeusistalking[.]com
	rgud-group[.]net

LEBANON-BASED CIB NETWORK

Tactic	Threat indicator
Acquiring assets	
Acquiring Facebook accounts	15 accounts
Acquiring Facebook Pages	5 Pages
Acquiring Instagram accounts	6 accounts
Acquiring domains to support influence operations	dofek[.]tv
	hahalom[.]com
Acquiring TikTok accounts	tiktok[.]com/@israel.in.a.minute
	tiktok[.]com/@dofektv
Acquiring X / Twitter accounts	twitter[.]com/israelinamin
	twitter[.]com/dofek_tv
Acquiring Youtube Channels	youtube[.]com/@IsraelinaMinute-in1zg
	youtube[.]com/channel/UCLC1nH7Df-piVzMWhoFYupw
Acquiring other social media assets	linktr[.]ee/israelinaminute
Disguising Assets	
Adopting visual disguise	Some of the accounts in the operation used profile photos likely generated using artificial intelligence such as Generative Adversarial Networks (GAN)

Posing as non-existent person	A fictitious journalist persona account was detected and disabled by automation as part of this network
Creating fictitious news outlet	The operation created three fictitious news entities called Dofek, Israel in a Minute, and Halalom Israel
Indiscriminate Engagement	
Posting common or generic hashtags	This network posted generic hashtags like #Israel, #Jerusalem, #Netanyahu among others.
Targeted Engagement	
Running Ads	Around $9,000 in spending for ads on Facebook and Instagram, paid for mostly in US dollars.
Engaging with users outside the operation	About 5,000 accounts followed one or more of these Pages
	About 5,200 accounts followed one or more of these Instagram accounts.
Engaging with specific audience	This network posted original content in Hebrew about news and geopolitical events in Israel

CONTINUOUS ENFORCEMENT: 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 may 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 BRANDS

This section includes the latest domains that we've identified as part of the Doppelganger campaign as of October 31, 2024. We have not seen new spoofed websites involved in activity on our services since our last update, but we have identified new iterations of Doppelganger's website brands. In addition to these domains, we've identified a few hundred more urls that the campaign uses to redirect people to its spoofing and branded 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
50statesoflie[.]so	9/6/2024	USA
artichoc[.]cc	9/5/2024	France
levinaigre[.]so	9/5/2024	France
lexomnium[.]pw	9/5/2024	France
rrn[.]so	9/5/2024	Global
holylandherald[.]pw	9/5/2024	Israel
ukrlm[.]so	9/5/2024	Ukraine
acrosstheline[.]cc	9/5/2024	USA
honeymoney[.]to	9/5/2024	USA
mypride[.]pw	9/5/2024	USA
shadowwatch[.]co	9/5/2024	USA
truthgate[.]so	9/5/2024	USA
uschina[.]cc	9/5/2024	USA
warfareinsider[.]cc	9/5/2024	USA

grenzezank[.]to	9/12/2024	Germany
lebelligerant[.]online	7/23/2024	France
lesifflet[.]online	7/23/2024	France
derbayerischelowe[.]online	7/23/2024	Germany
holylandherald[.]online	7/23/2024	Israel
polemix[.]online	7/23/2024	Poland
laterrasse[.]io	7/13/2024	France
lebelligerant[.]io	7/13/2024	France
lesifflet[.]cc	7/13/2024	France
brennendefrage[.]cc	7/13/2024	Germany
deintelligenz[.]io	7/13/2024	Germany
derleitstern[.]cc	7/13/2024	Germany
derrattenfanger[.]io	7/13/2024	Germany
kaputteampel[.]cc	7/13/2024	Germany
il-corrispondente[.]io	7/13/2024	Italy
alhiwar[.]cc	7/13/2024	Middle East
polemix[.]cc	7/13/2024	Poland
cropmarketchronicles[.]cc	7/13/2024	USA
electionwatch[.]io	7/13/2024	USA
interventionist[.]cc	7/13/2024	USA
liesofwallstreet[.]io	7/13/2024	USA
spicyconspiracy[.]io	7/13/2024	USA
uschina[.]online	7/13/2024	USA
la-sante[.]press	7/11/2024	France
le-continent[.]press	7/11/2024	France
hauynescherben[.]press	7/11/2024	Germany
omnam[.]media	7/11/2024	Israel
meisterurian[.]to	10/14/2024	Germany