Russian disinformation network's infrastructure is spread across Europe, report says

By Daryna Antoniuk

Published: 2024-07-11 · Archived: 2026-04-05 13:14:39 UTC

Researchers have uncovered infrastructure located or registered in Europe that is used by a prolific Russian-language disinformation network dubbed Doppelgänger, as well as by cybercriminals.

Researchers at digital rights nonprofits Qurium and EU DisinfoLab — who first exposed Doppelgänger in 2022 — say the group is doing business in at least 10 countries across Europe, including Germany, the U.K., and the Czech Republic.

This means that European companies, whether knowingly or not, make their services available to a disinformation operation affecting their own nations, researchers said.

Doppelgänger has been operating in Europe since at least May 2022. It is known for spreading fake articles on websites that resemble the design of real media outlets such as Germany's Der Spiegel and Britain's The Guardian.

The network's goal is to advance the interests of the Kremlin and sow discord among its enemies, including the U.S. and Western Europe.

The researchers spent several months tracking Doppelgänger's activity, by tracing the path an internet browser takes when a targeted user clicks on one of the fake news sites.

According to German nonprofit journalism group Correctiv, which was involved in the investigation, an early version of the Qurium report has been circulating since spring this year among government agencies in at least two European countries, including Germany.

"However, the information has apparently not been used to put a stop to the campaign," Correctiv said. This "raises the question of how seriously European authorities are fighting disinformation," they added.

Foreign infrastructure

Doppelgänger registered dozens of legal entities in the U.K., often in the names of young Russian citizens, in order to build the propaganda campaigns and obscure its alleged Russian origins, researchers said.

One such company, TNSecurity, with a virtual office in London, is home to hundreds of malicious web domains, the report said. It also provides services to cybercriminals who buy stolen credit cards or bank accounts.

According to an earlier report by security company Hyas, TNSecurity "may have been compromised or willingly collaborating with cybercriminals."

At the core of Doppelgänger's operation in Europe and Russia is a company called Aeza — a Saint Petersburg-based hosting service provider. Aeza allows suspected criminals to operate on its own servers and usually finds its clients on the darknet, researchers said. For example, the company likely provides its services to the operators of the malware infrastructures known as Lumma and Meduza.

Some of the European hosting companies identified in the report are direct or hidden branches of Aeza.

For example, the Frankfurt-based IT company Aurologic partly runs data traffic for TNSecurity and other companies associated with Aeza, according to the research. The owner of Aurologic told Correctiv that he knows nothing about Doppelgänger and that the German authorities have not made any complaints against him.

The technical infrastructure of Doppelgänger is "extensive," researchers say, comprising more than 300 network prefixes and 100,000 IP addresses with a market value of €5 million or a leasing cost of approximately €50,000 a month.

"This massive infrastructure investment can only be sustained by serious financial support from external actors," the report said.

Recorded Future News reached out to several hosting providers mentioned in the report but had not received a response as of the time of publication.

No previous article

No new articles

Daryna Antoniuk

is a reporter for Recorded Future News based in Ukraine. She writes about cybersecurity startups, cyberattacks in Eastern Europe and the state of the cyberwar between Ukraine and Russia. She previously was a tech reporter for Forbes Ukraine. Her work has also been published at Sifted, The Kyiv Independent and The Kyiv Post.
