Russia's largest platform for state procurement hit by cyberattack from pro-Ukraine group
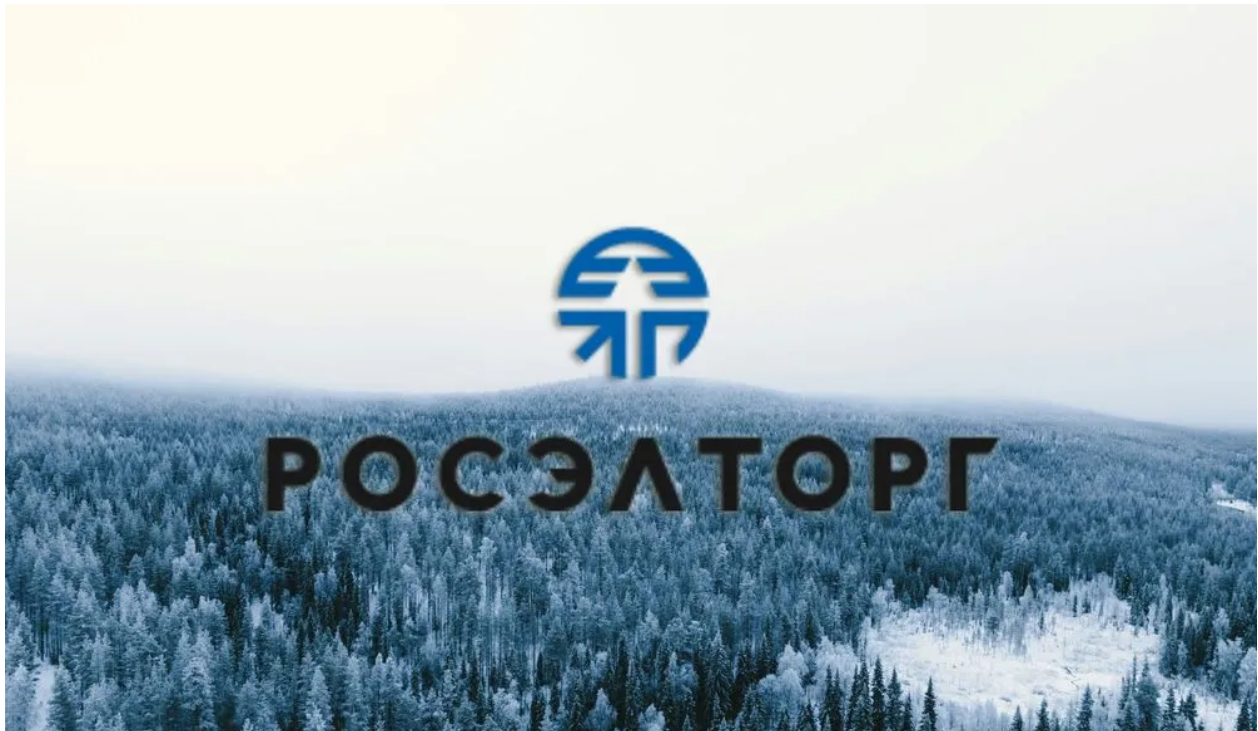
Image: Unsplash+/Roseltorg

[Daryna Antoniuk](#)

January 14th, 2025

Russia's main electronic trading platform for government and corporate procurement confirmed on Monday that it had been targeted by a cyberattack after initially claiming that outages were caused by "maintenance work."

Roseltorg is one of the largest electronic trading operators selected by the Russian government to conduct public procurement, including contracts in the defense and construction industries. The platform also offers tools for electronic document management and procurement planning.

The company initially confirmed last Thursday that its services had been temporarily suspended, without providing further details. In a recent Telegram statement, Roseltorg disclosed that it had been targeted by "an external attempt to destroy data and the entire infrastructure of electronic trading."

Roseltorg stated that all data and infrastructure affected by the recent attack had been fully restored, and trading systems are expected to resume operations shortly. However, as of the time of writing, the company's website remains offline.

Last week, the previously unknown pro-Ukraine hacker group Yellow Drift claimed responsibility for the attack on Roseltorg, stating they had deleted 550 terabytes of data, including emails and backups. As proof, the hackers published screenshots from the platform's allegedly compromised infrastructure on their Telegram channel.

"If you support tyranny and sponsor wars, be prepared to return to the Stone Age," the hackers said.

The cyberattack on Roseltorg is already impacting clients who rely on the platform's operations, including government agencies, state-owned companies and suppliers. Following the company's announcement, many clients expressed concerns in the comments section, complaining about potential financial losses and delays in the procurement process.

Roseltorg said in a statement that once access to the trading systems is reinstated, all deadlines for procedures, including contract signings, will be automatically extended without requiring any requests from users.

According to local media reports, Roseltorg serves some of the largest Russian corporations, including oil company Lukoil, digital service provider Rostelecom and diamond mining company Alrosa, as well as government agencies such as the Ministry of Defense and internet regulator Roskomnadzor.

Roseltorg is one of several Russian companies targeted by pro-Ukraine hackers this month. Last week, a group of hackers with unknown ties claimed responsibility for breaching Rosreestr, a Russian government agency responsible for managing property and land records.

Another hacker group known as the Ukrainian Cyber Alliance also claimed responsibility for an attack on the Russian internet provider Nodex, stating that it destroyed the company's infrastructure overnight. Nodex confirmed the attack.

On Monday, a Ukrainian hacker group called <u>Cyber Anarchy Squad</u> announced it had attacked the Russian tech company Infobis, which develops systems for planning, monitoring, and accounting of agricultural work. The hackers claimed to have exfiltrated three terabytes of information and destroyed part of the company's infrastructure. Infobis has not commented on the alleged attack.

- <u>Cybercrime</u>
- <u>Government</u>
- <u>News</u>
- <u>Technology</u>

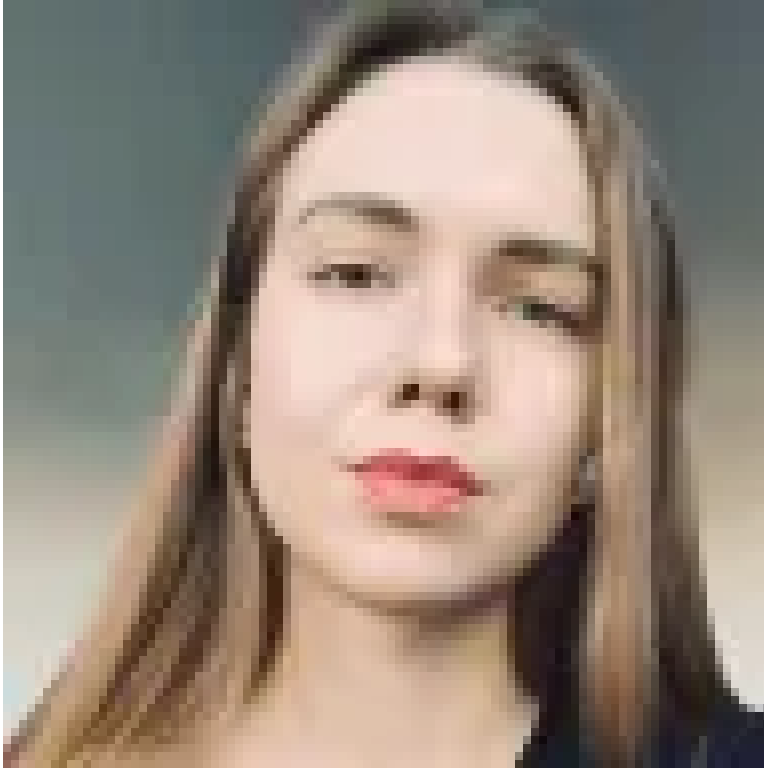Get more insights with the
Recorded Future

Intelligence Cloud.

<u>Learn more.</u>
Tags
- <u>data breach</u>
- <u>Cyberattack</u>
- <u>Russia</u>
- <u>Ukraine</u>
- <u>government portal</u>

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.