French Cyber Agency Warns of APT28 Hacks Against Think Tanks

By Akshaya Asokan

Archived: 2026-04-05 23:38:17 UTC

Cyberwarfare / Nation-State Attacks , Fraud Management & Cybercrime

Report: North Korean, Russian, Chinese, Iranian Actors Are Targeting Research Orgs (asokan_akshaya) • September 11, 2024

Russian state hackers are targeting Western think tanks, warned the French cyber defense agency. (Image: Shutterstock)

Russian state hackers who are part of Moscow intelligence gathering operations are targeting think tanks studying strategic interests and the defense sector, warned the French cyber agency.

See Also: Experts Offer Insights from Theoretical to the Realities of AI-enabled Cybercrime

In a Tuesday report evaluating threats to global think tanks, the French National Agency for Information Systems Security said nation-state actors tied to North Korea, Russia, China and Iran are the top threats to research organizations worldwide.

Although cyberattacks have been ongoing for years, Western think tanks specializing in defense and international relations have witnessed an influx of attacks, especially tied to Russian state hackers, following the Kremlin's invasion of Ukraine in February 2022, ANSSI said.

"In the context of growing tensions between Russia and NATO member countries, this sector represents a constant interest for attackers seeking strategic information on geopolitical and defense issues," the report says, adding that the attacks are part of Russia's military espionage campaigns.

A hacking group that officially is Unit 26165 of the Russian Main Intelligence Directorate - and tracked variously as APT28, Forest Blizzard and Fancy Bear - appears to be Russia's most prolific targeter of think tanks.

Victims include several French researchers, as well as an unidentified French strategic institute that weathered phishing attacks that intended to steal sensitive employee details, ANSSI said.

Also known as Pawn Storm, the group is known for complex operations that steal victims' credentials to enable surveillance or intrusion operations.

The German Federal Office for Information Security earlier this month disclosed an investigation into an apparent APT28 hacking campaign that used a domain mimicking the Kiel Institute for the World Economy, a German think tank (see: *German Cyber Agency Investigating APT28 Phishing Campaign*).

"The case underlines that NGOs and scientific institutions are potential targets for cyberattacks. We are taking this threat seriously, and are in regular contact with the authorities," a Kiel Institute spokesperson told Information Security Media Group.

"Russian cyber operations are deeply intertwined with its broader foreign policy objectives," said Eugenio Benincasa, a cybersecurity researcher at ETH Zurich. He said Moscow's espionage activities are part of its "hybrid warfare" approach that blends cyber tactics with political interference, economic pressure, and military threats.

"By employing these low-cost, high-impact methods, Russia aims to exert influence, shape public opinion and destabilize key NATO and EU member states supporting Ukraine," Benincasa said.
