

GERMANY AND CZECHIA ATTRIBUTE APT28 CAMPAIGN INCL. SPD HACK TO GRU

On 3 May 2024, Germany and Czechia attributed to GRU-linked APT28 a cyber campaign that exploited an Outlook vulnerability. In Germany, the campaign hit the SPD party headquarters from late December 2022, along with defence, logistics, aerospace and IT firms. Czech state institutions were also targeted. The EU and NATO issued supporting statements.

UKRAINE EVIDENCE HUB
BEYOND UKRAINE
AS OF 15 OCT 2026

DEGREE OF PROOF

OFFICIAL ATTRIBUTION

A government, a prosecutor, the EU, NATO or a UN body has formally named Russia, its services or its state-backed forces. This is a position of that authority, not a verdict.

WHO ESTABLISHED IT

German Federal Government / Federal Ministry of the Interior (3 May 2024); Czech Ministry of Foreign Affairs (3 May 2024); EU High Representative and NATO statements the same day.

LATEST

Germany has since attributed further APT28 operations, including the August 2024 attack on air traffic control provider DFS (Dec 2025).

LINK TO THE WAR AGAINST UKRAINE

The German government links the timing of the campaign to its support for Ukraine (start of 2023).

SOURCES

B German Federal Ministry of the Interior – Cyber attacks traced to Russian military intelligence agency · 2024-05-03

<https://bmi.bund.de/SharedDocs/kurzmeldungen/EN/2024/05/schutzmassnahmen-cyberangriffe-en.html>

B Czech Ministry of Foreign Affairs – Statement of the MFA on the cyberattacks · 2024-05-03

https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/statement_of_the_mfa_on_the_cyberattacks.html

C Security Affairs – NATO and the EU formally condemned Russia-linked APT28 cyber espionage · 2024-05-03

<https://securityaffairs.com/162759/apt/nato-eu-condemned-apt28-espionage.html>

WHAT WE ASK OF MEMBER STATES

- Attribute jointly and raise it in the UN Open-ended Working Group on ICT security.
- Use the EU cyber sanctions regime against the units responsible.
- Share indicators and support the resilience of critical infrastructure.

Status follows four degrees of proof: court finding · official attribution · charged · suspected (suspected cases are listed only on the live page). Tier A = courts, UN bodies, international organisations · B = governments, prosecutors · C = media and investigators. Corrections: evidence@ukraine-evidence.org



live page · corrections