German Cyber Agency Investigating APT28 Phishing Campaign

By Akshaya Asokan

Archived: 2026-04-05 13:02:53 UTC

Cyberwarfare / Nation-State Attacks , Fraud Management & Cybercrime

Der Spiegel Reports Russian State Hackers Mimicked Kiel Institute (asokan_akshaya) • September 9, 2024

Russian APT28 hackers mimicked the Kiel Institute for the World Economy. (Image: Kiel Institute)

The German cyber agency is reportedly investigating a phishing campaign tied to Russian state hacking group APT28 that used a bogus website mimicking an influential think tank.

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

Citing a confidential IBM X-Force report, German publication Der Spiegel on Friday said the group created a domain mimicking Kiel Institute for the World Economy.

The campaign, which ran for months, used variations of the institute's legitimate `ifw-kiel` web domain to lure victims. When targets visited a fake site, they saw a blurry official document containing instructions to click further to read. Clicking started a chain of loading malware on victim computers. Der Spiegel reported that it's unclear whether the Kiel Institute was the target of the attack or whether hackers used its reputation as bait.

A spokesperson for the German BSI did not immediately respond to a request seeking clarification. It told Der Spiegel it is investigating the campaign.

News of the phishing campaign comes just days after the BSI joined the U.S. and other state cyber agencies to disclose details of a long-standing APT28 campaign using WhisperGate wiper. The variant has been used by the group to target Ukrainian and Western nations' critical infrastructure since the Russian war against Ukraine began (see: *US Broadens Indictments Against Russian Intelligence Hackers*).

Also known as Forest Blizzard, Fancy Bear and Pawn Storm, APT 28 is part of the Russian Main Intelligence Directorate. A U.S. federal indictment of 12 GRU officials in July 2018 identifies the threat actor as Unit 26165 of the GRU.

The German Federal Ministry of the Interior and Community in May attributed a hacking campaign that targeted the members of the German Social Democratic Party to APT28 (see: *Russian GRU Hackers Compromised German, Czech Targets*).

In a move intended to shore up its defense capabilities in the wake of increased cyberattacks, German Defense Minister Boris Pistorius recently announced plans to revamp the country's military forces, which includes creating a new force that specializes in electronic warfare and cyberwarfare.
