North Korea Hackers Linked to Breach of German Missile Manufacturer

By Ryan Naraine

Published: 2024-09-30 · Archived: 2026-04-02 11:58:53 UTC

A professional hacking team linked to the North Korean government has broken into Diehl Defence, a German company that manufactures Iris-T air defense systems, using a clever phishing campaign with fake job offers and advanced social engineering tactics, according to a report by *Der Spiegel*.

The attack, pinned on the Kimsuky APT, combined the use of booby-trapped PDF files with spear-phishing lures offering Diehl Defence employees jobs with American defense contractors.

The targeting of Diehl Defence is significant because the company specializes in the production of missiles and ammunition. Last October, Diehl Defence inked a deal to supply South Korea with its Iris-T short-range air-to-air missiles.

According to the Der Spiegel report, researchers at Mandiant investigated the compromise and found the attackers performed detailed reconnaissance on Diehl Defense ahead of the spear-phishing attacks.

Der Spiegel reported that the Kimsuky hackers hid their attack server behind an address containing “Uberlingen,” a reference to Diehl Defence’s location in Überlingen in Southern Germany.

The attack server also hosted authentic-looking, German-language login pages that resembled those of telecommunications provider Telekom and email service GMX, suggesting the attackers were bulk-harvesting login credentials of German users.

Mandiant could not be reached for comment on the report.

Kimsuky, also known as APT43, Velvet Chollima, Emerald Sleet, TA406, and Black Banshee, focuses on intelligence gathering, including in support of Pyongyang's nuclear and strategic efforts.

The threat group has been known to target governments, think tanks, research centers, universities, and news organizations in the United States, Europe and Asia.

The US government has slapped sanctions on individuals associated with Kimsuky and issued multi-agency advisories with technical details on the group's hacking activities.

Related: US Sanctions North Korean Cyberespionage Group Kimsuky

Related: North Korea Kimsuky Targets Government Agencies With New Malware

Related: U.S. Shares Information on North Korean Threat Actor 'Kimsuky'

Related: Microsoft Catches APTs Using ChatGPT for Malware Scripting

Related: Inside the APT Behind North Korea's Digital Military Machine

---