North Korean hackers stole anti-aircraft system data from South Korean firm

By James Reddick

Published: 2023-12-06 · Archived: 2026-04-05 21:54:06 UTC

The Seoul Metropolitan Police on Tuesday accused a North Korean hacking group of targeting South Korean companies connected to the defense industry and stealing sensitive information about anti-aircraft weapon systems.

In a press release publicizing the investigation into the Andariel hacking group — which has links to the notorious Lazarus Group — police said they seized servers in South Korea used by the group, conducted forensic searches of cellphones and laptops, and had searched the residence of a "foreign" woman accused of laundering the proceeds of ransomware attacks.

The investigation was conducted alongside the FBI.

Andariel is connected to North Korea's intelligence office, the Reconnaissance General Bureau, which also houses Lazarus Group, according to government officials. The group was sanctioned in 2019 by the U.S. Treasury, which said the group "consistently executes cybercrime to generate revenue and targets South Korea's government and infrastructure in order to collect information and to create disorder."

According to Seoul investigators, the hackers specifically targeted defense companies — stealing "technical data" on anti-aircraft systems — as well as research institutes and pharmaceutical companies.

They determined that 1.2 terabytes of data had been stolen in attacks and notified the relevant companies, some of which were unaware they had been targeted. Others had contacted police when they discovered a breach, while in some cases "damage was not reported" to authorities.

The hackers allegedly used a South Korean domestic server rental company as a "base for hacking," with 83 connections made from a part of downtown Pyongyang where the International Telecommunications Bureau is housed.

Investigators tracked paid ransoms on the cryptocurrency platforms Binance and Bithumb, including about $76,000 transferred into an account at a Chinese bank, where the funds were taken out at a branch close to the border with North Korea.

Separately, investigators found the group extorted three ransomware victims in South Korea and abroad for about $357,000 worth of Bitcoin.

Last month, the United Kingdom and South Korea issued a joint advisory warning of supply-chain attacks carried out by North Korean hackers. Also in November, the U.S., Japan and South Korea agreed to convene a consultative body on a quarterly basis for the purpose of "jointly preparing measures to block cyber activities that

are abused as a major source of funds for North Korea's weapons development, such as nuclear weapons and WMD," the South Korean government said.

No previous article

No new articles

James Reddick

has worked as a journalist around the world, including in Lebanon and in Cambodia, where he was Deputy Managing Editor of The Phnom Penh Post. He is also a radio and podcast producer for outlets like Snap Judgment.
