South Korea says DPRK hackers stole spy plane technical data

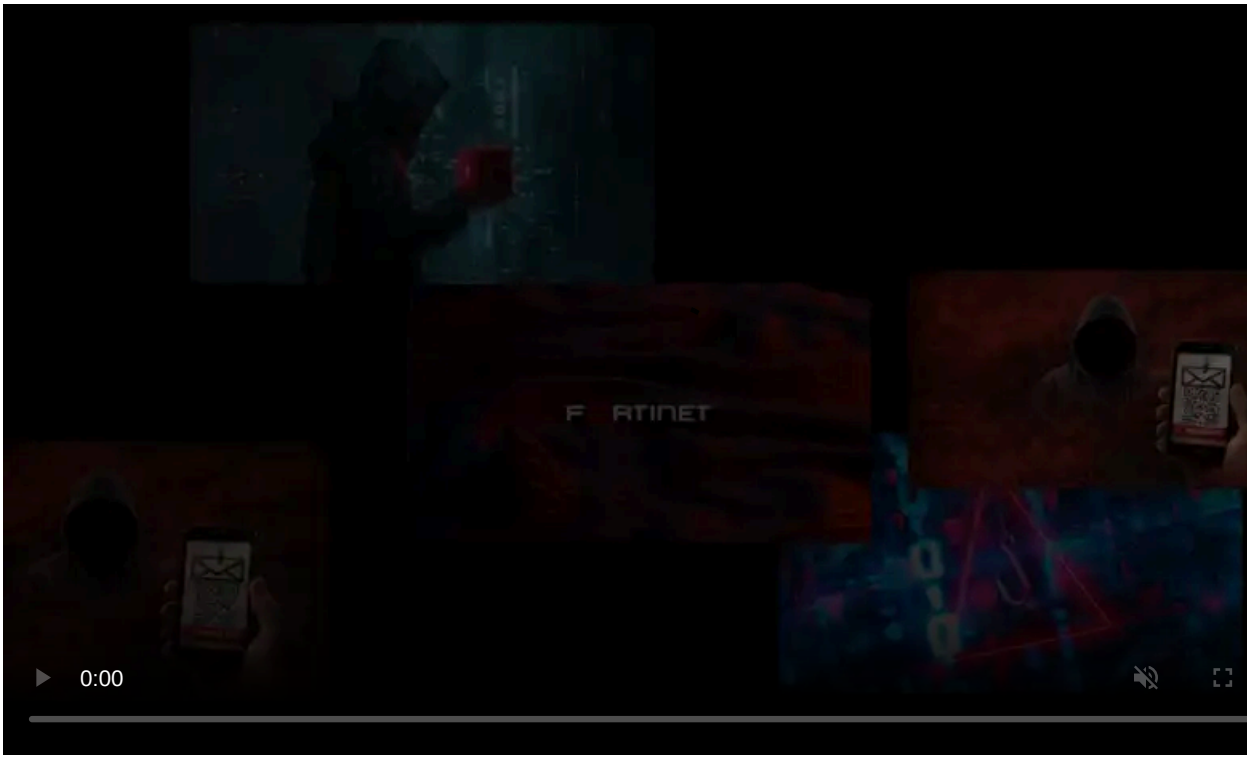
By Bill Toulas

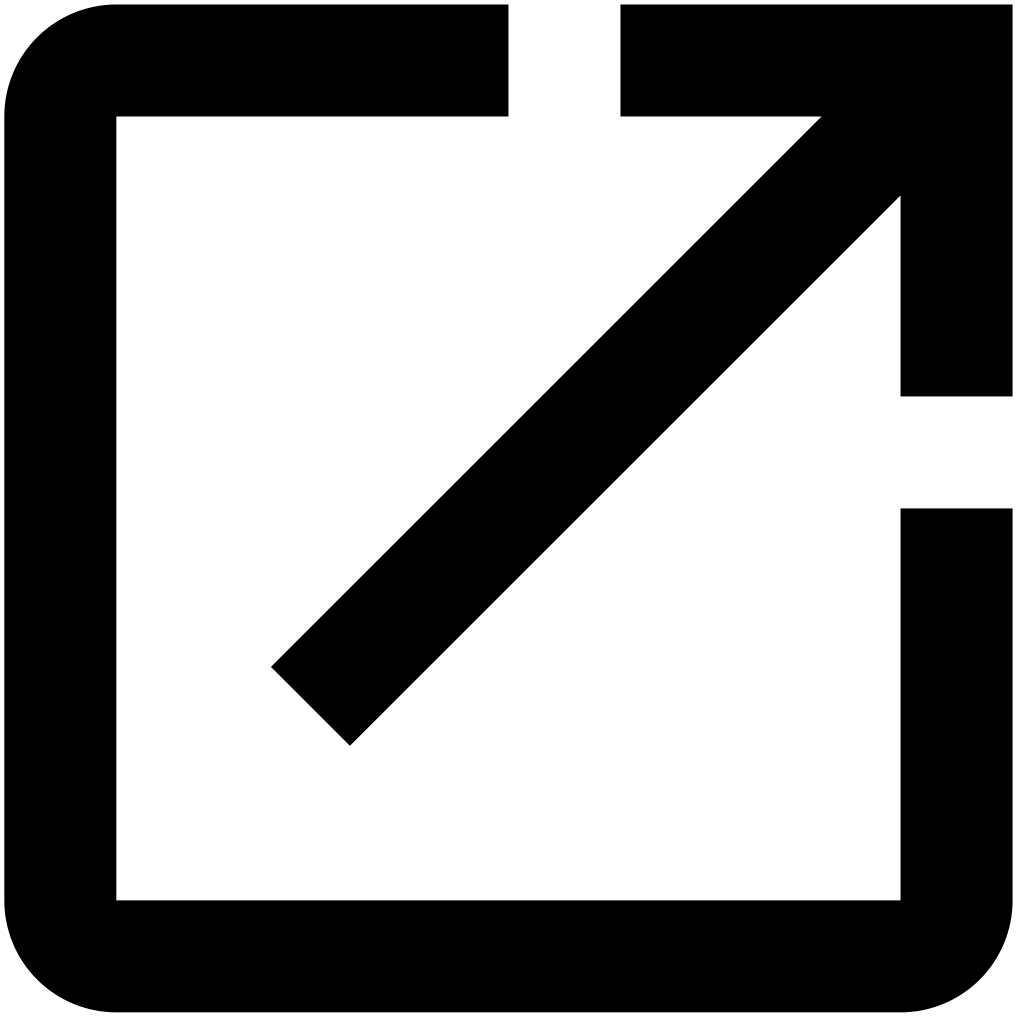
Published: 2024-08-12 · Archived: 2026-04-06 03:23:39 UTC

South Korea's ruling party, People Power Party (PPP), claims that North Korean hackers have stolen crucial information about K2 tanks, the country's main battle tank, as well as its "Baekdu" and "Geumgang" spy planes.

PPP fears that DPRK will use this information to evade military surveillance and gain an advantage on the battlefield, so it's calling for the urgent introduction of stronger measures to safeguard national security.

K2 "Black Panther" is a South Korean tank designed by the Agency for Defense Development and built by Hyundai Rotem. It was introduced in 2008, costs $8.5 million per unit, and it's the country's main battle tank, with 260 units currently in service and another 150 in plans.


F RTINET
0:00



Baekdu and Geumgang are spy plains South Korea has heavily used for border surveillance in the past 20 years, monitoring North Korea's military activities (IMINT), and capturing wireless communications (SIGINT).

According to local media reports from Friday, the leakage of the K2 tank data occurred when engineers working on one of the tank's part makers moved to a competing company, taking along with them in external storage drives design blueprints, development reports, and details about the tank's overpressure system.

Their new employer attempted to export this technology to a Middle Eastern country, so the leak is thought to have extended beyond South Korea.

Regarding Baekdu and Geumgang, Donga reported that a South Korean defense contractor which produces operational and maintenance manuals for military equipment, including the two spy planes, was hacked by North Koreans.

The hackers stole significant technical data about the two planes, including details about their technology and recent technical upgrades, operation capabilities, and maintenance information.

Calls for increased cybersecurity

South Korea is worried that the theft of its surveillance aircraft technology would allow its enemies to develop stealthier drones and effective surveillance evasion measures.

PPP calls on all political parties in the country to leave their differences aside and agree on new measures that should be introduced immediately. These measures will bolster the country against cyber-espionage operations.

"Moreover, as North Korea's cyberattacks become more widespread and bold by the day, enacting the Basic Cyber Security Act to prevent North Korea's hacking and technology theft is no longer an option but a necessity," reads the PPP statement.

"In addition, in order to protect our national interests, we must quickly pursue a revision of the criminal law that expands the scope of application of espionage laws to ‘foreign countries.’ "

In April 2024, the National Police Agency in South Korea issued an urgent warning to alert defense industry firms about elevated targeting by notorious North Korean threat groups, including Lazarus, Andariel, and Kimsuky.

The police conducted a special clean-up operation where it discovered that DPRK operatives had compromised multiple companies since late 2022, allowing the attackers ample time to perform extensive intelligence collection.

Source: https://www.bleepingcomputer.com/news/security/south-korea-says-dprk-hackers-stole-spy-plane-technical-data/