North Korean hackers breached major hospital in Seoul to steal data

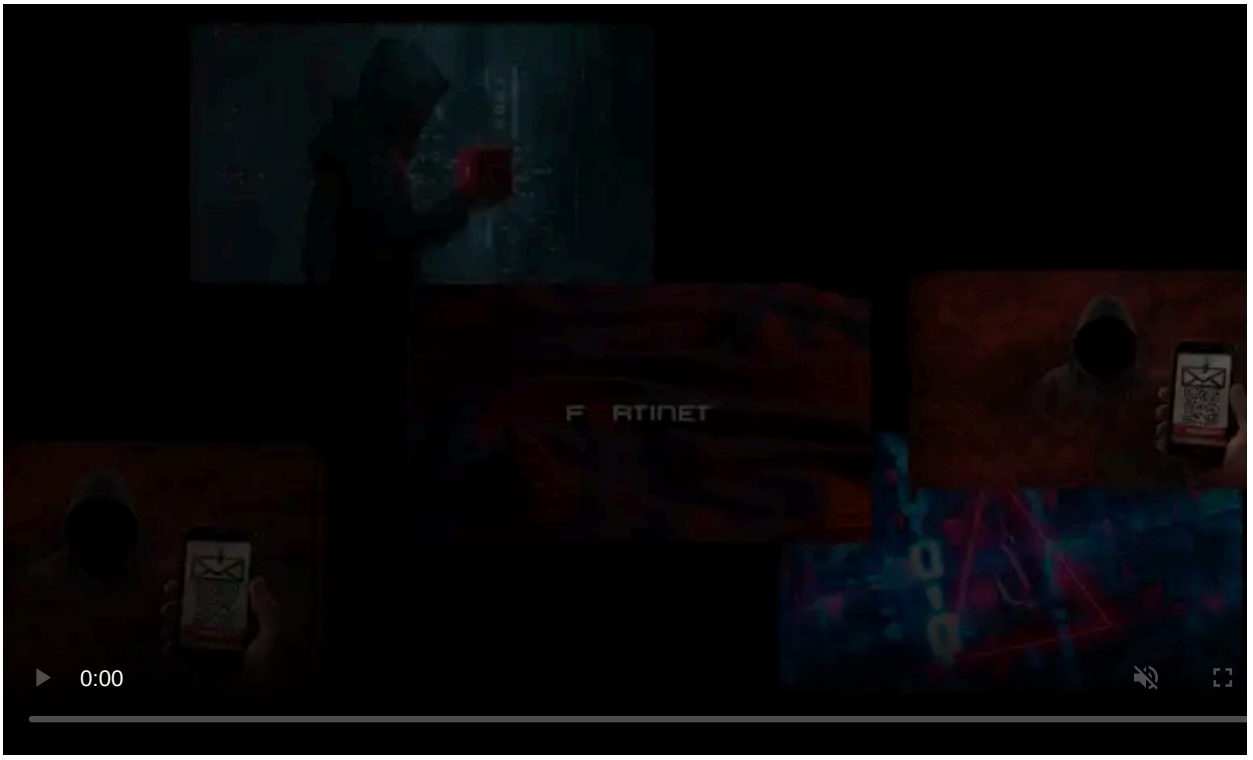
By Bill Toulas

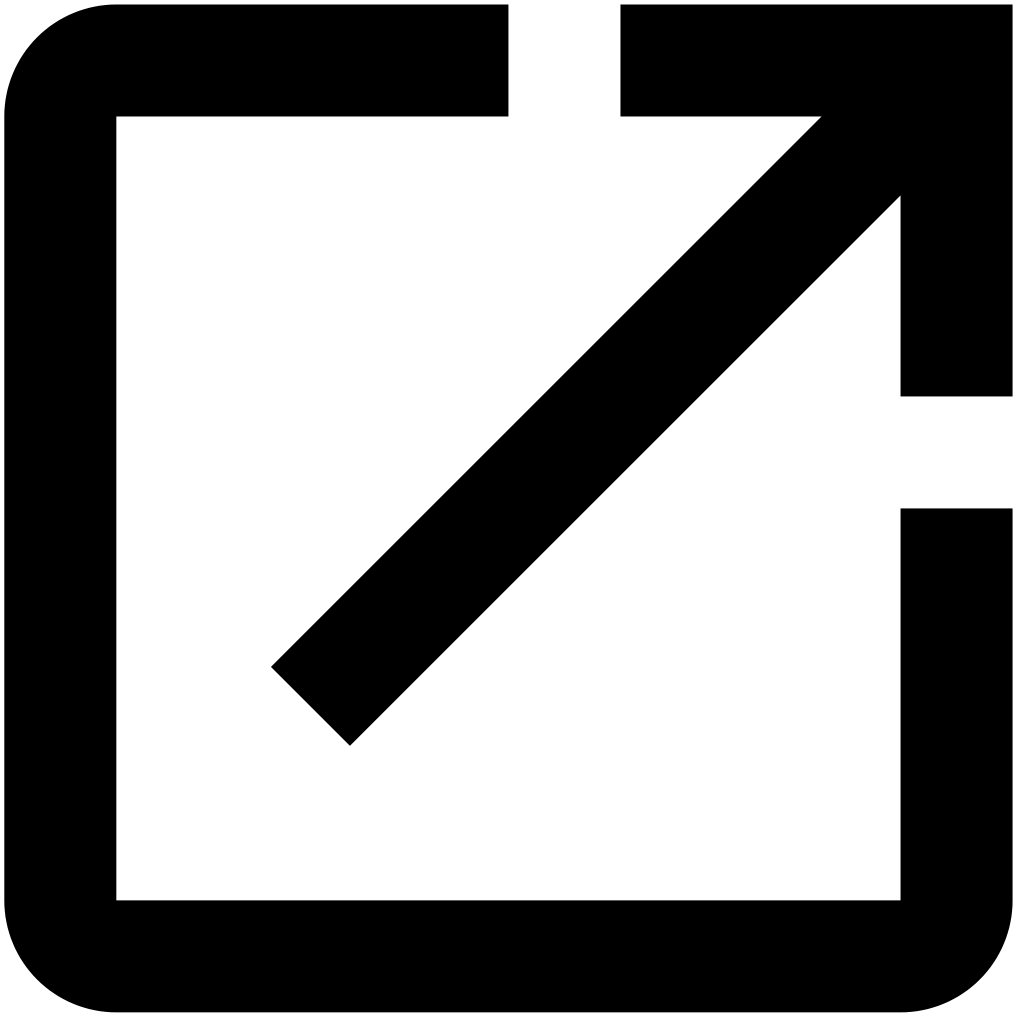
Published: 2023-05-10 · Archived: 2026-04-05 20:46:16 UTC

The Korean National Police Agency (KNPA) warned that North Korean hackers had breached the network of one of the country's largest hospitals, Seoul National University Hospital (SNUH), to steal sensitive medical information and personal details.

The incident occurred between May and June 2021, and the police conducted an analytical investigation during the past two years to identify the perpetrators.

According to the law enforcement agency's press release, the attack was attributed to North Korean hackers based on the following information:

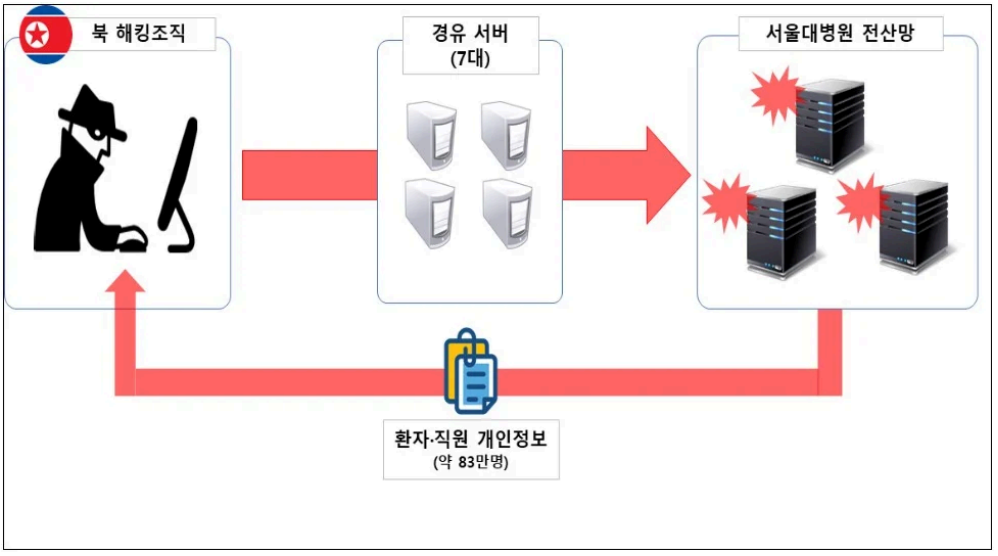

0:00



- the intrusion techniques observed in the attacks,
- the IP addresses that have been independently linked to North Korean threat actors,
- the website registration details,
- the use of specific language and North Korean vocabulary

Local media in South Korea linked the attack to the Kimsuky hacking group, but the police's report does not explicitly mention the particular threat group.

The attackers used seven servers in South Korea and other countries to launch the attack on the hospital's internal network.



Attack outline *(police.go.kr)*

The police said the incident resulted in data exposure for 831,000 individuals, most of whom were patients. Also, 17,000 of the impacted people are current and former hospital employees.

The KNPA press release cautioned that North Korean hackers might try to infiltrate information and communication networks across various industries. It emphasized the need for enhanced security measures and procedures, such as implementing security patches, managing system access, and encrypting sensitive data.

"We plan to actively respond to organized cyber-attacks backed by national governments by mobilizing all our security capabilities and to firmly protect South Korea's cyber security by preventing additional damage through information sharing and collaboration with related agencies," warned the KNPA.

Maui and Andariel

North Korean hackers have been previously linked to hospital network intrusions aiming to steal sensitive data and extort a ransom payment from healthcare organizations.

More specifically, the U.S. government has highlighted the Maui ransomware threat as such, warning the healthcare sector that they need to raise their defenses against the North Korean operation.

Soon after this warning, security researchers at Kaspersky linked the Maui ransomware operation to a specific cluster of activity named 'Andariel' (aka 'Stonefly'), believed to be a sub-group of Lazarus.

Lazarus is known for targeting South Korean entities with ransomware since April 2021.
