# DPRK hacking groups breach South Korean defense contractors

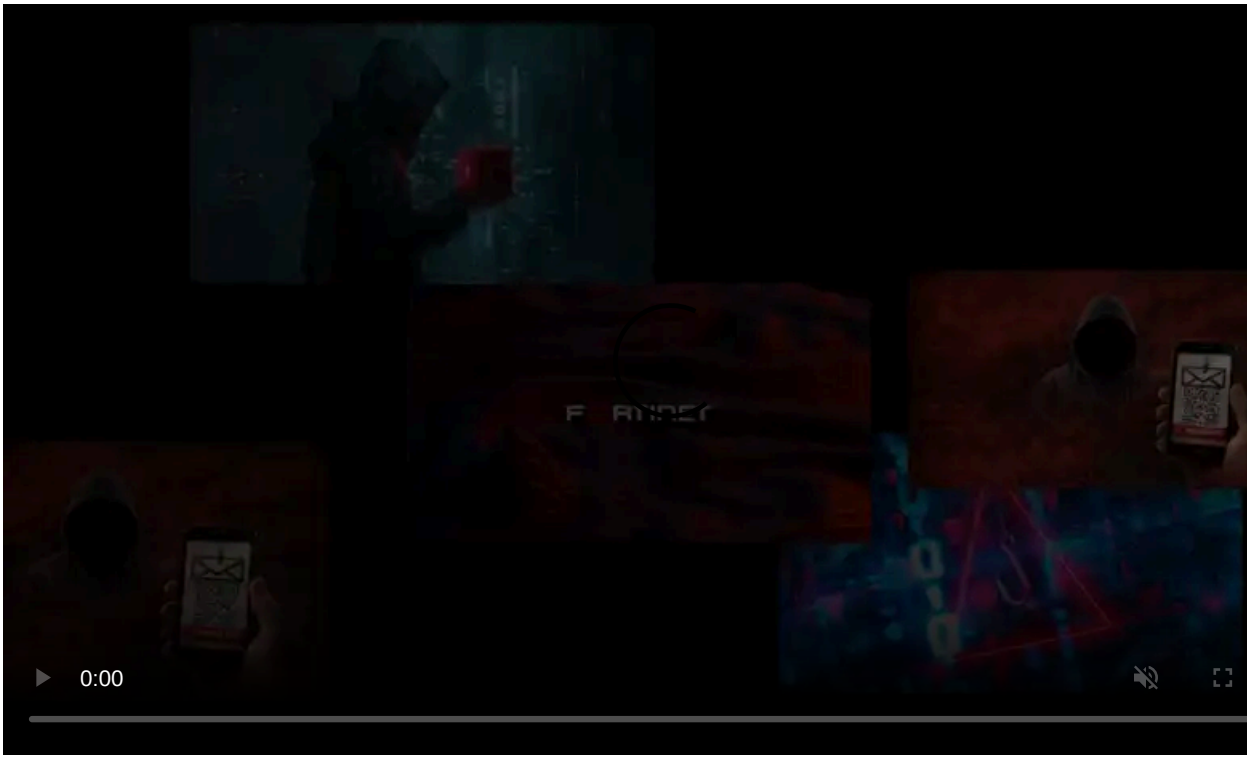
By Bill Toulas

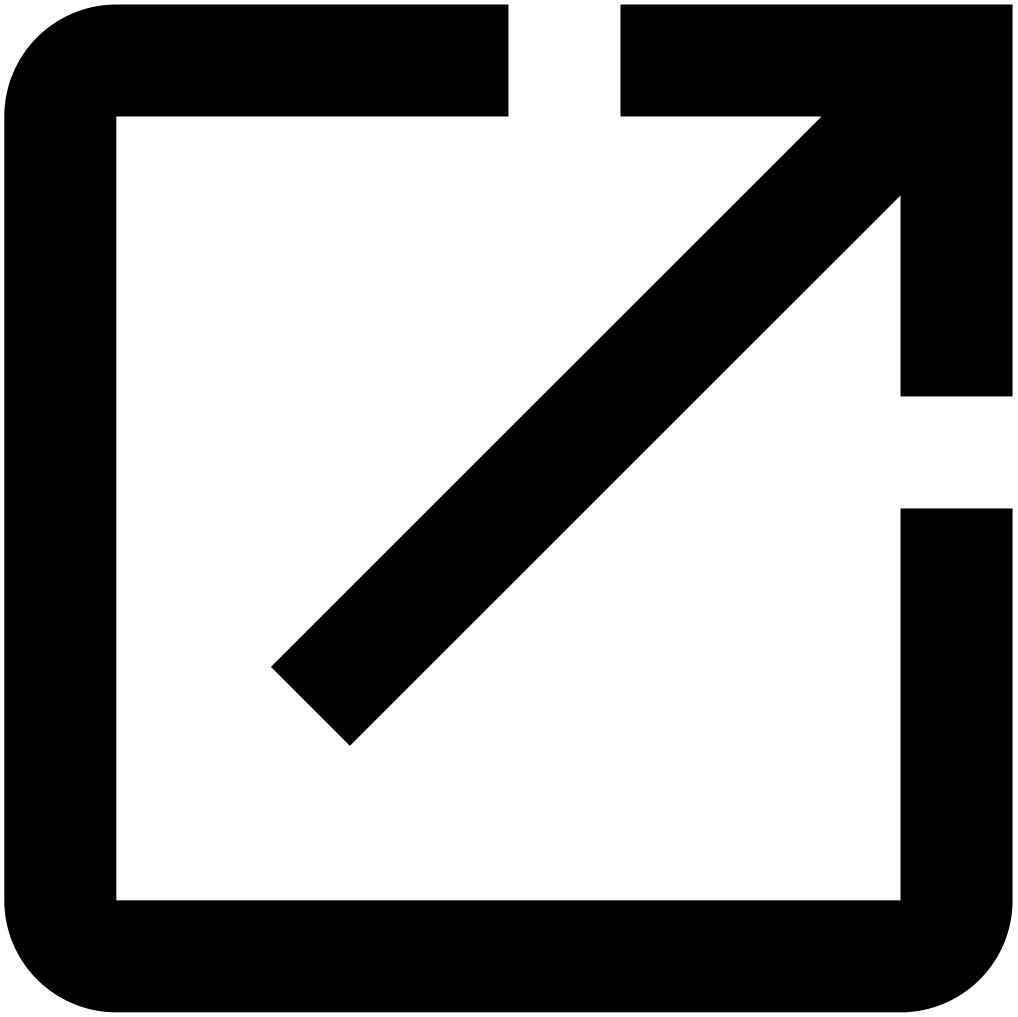
Published: 2024-04-23 · Archived: 2026-04-06 02:53:29 UTC

The National Police Agency in South Korea issued an urgent warning today about North Korean hacking groups targeting defense industry entities to steal valuable technology information.

The police discovered several instances of successful breaches of defense companies in South Korea involving the hacking groups Lazarus, Andariel, and Kimsuky, all part of the North Korean hacking apparatus.

According to the announcement, the attackers breached the organizations by leveraging vulnerabilities in targets' or their subcontractors' environments to plant malware capable to exfiltrate data.


0:00



The National Police Agency and the Defense Acquisition Program Administration conducted a special inspection earlier this year between January 15 and February 16 and implemented protective measures to secure critical networks.

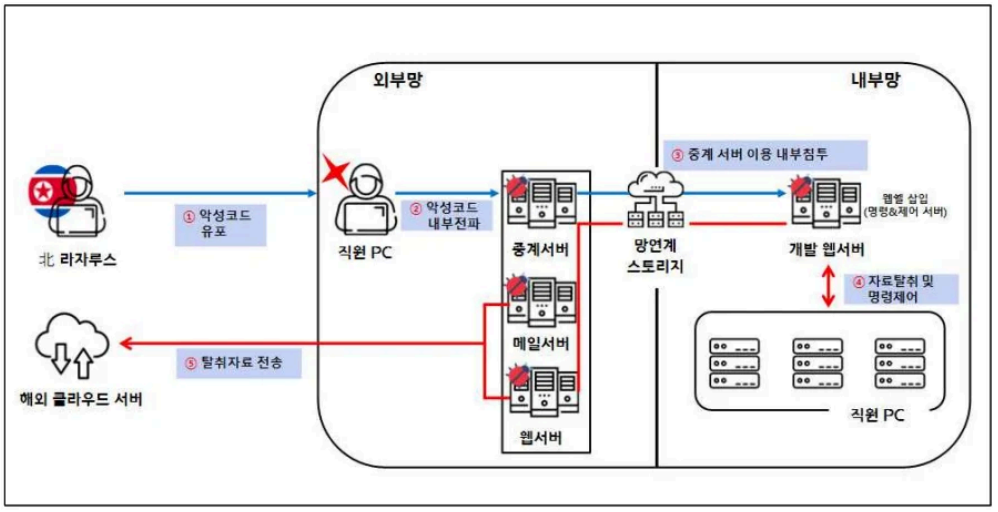
This special operation discovered multiple companies that had been compromised since late 2022 but were unaware of the breach until authorities informed them.

## Diverse attacks

The police report highlights three cases involving each of the mentioned hacking groups, displaying multi-faceted attack methods aimed at stealing defense tech.

Lazarus hackers exploited poorly managed network connection systems designed for testing and penetrated the internal networks of a defense company since November 2022.

After infiltrating the network, they gathered critical data stored in at least six of the firm's computers and transferred it to a cloud server abroad.



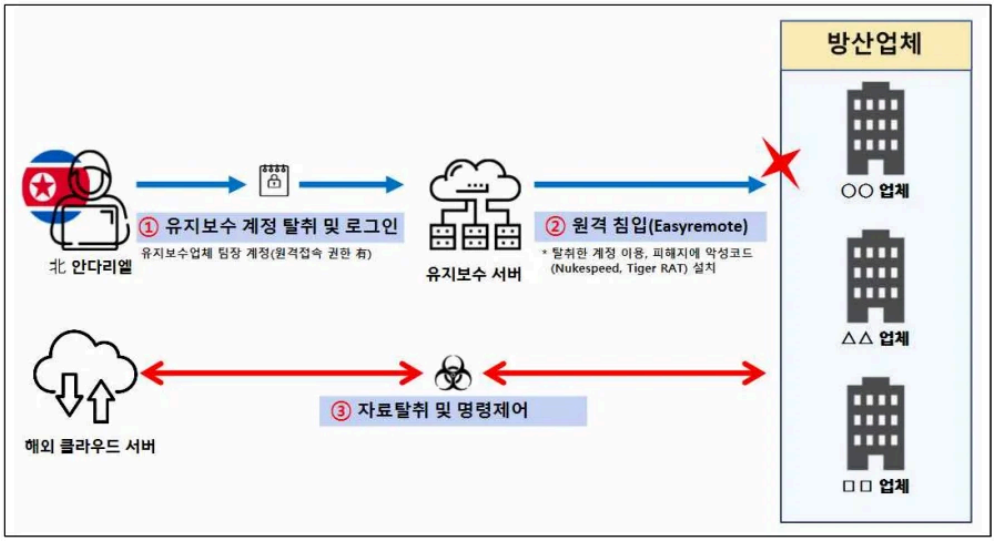

**Lazarus attack overview**

*Korean police*

The second attack was attributed to the Andariel group, who stole account information from an employee of a maintenance company that serviced defense subcontractors.

Using this stolen account in October 2022, they installed malware on the servers of these subcontractors, leading to significant leaks of defense-related technical data.

This network infiltration was further exacerbated by employees using the same passwords for personal and work accounts.

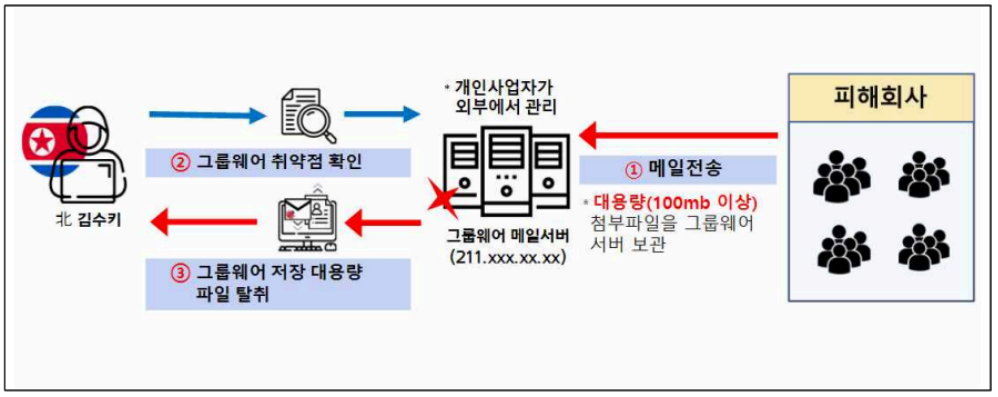



**Andariel attack overview**

*Korean police*

A third attack highlighted in the police's advisory, Kimsuky exploited a vulnerability in the email server of a defense subcontractor between April and July 2023, which allowed large files to be downloaded without the need to authenticate.

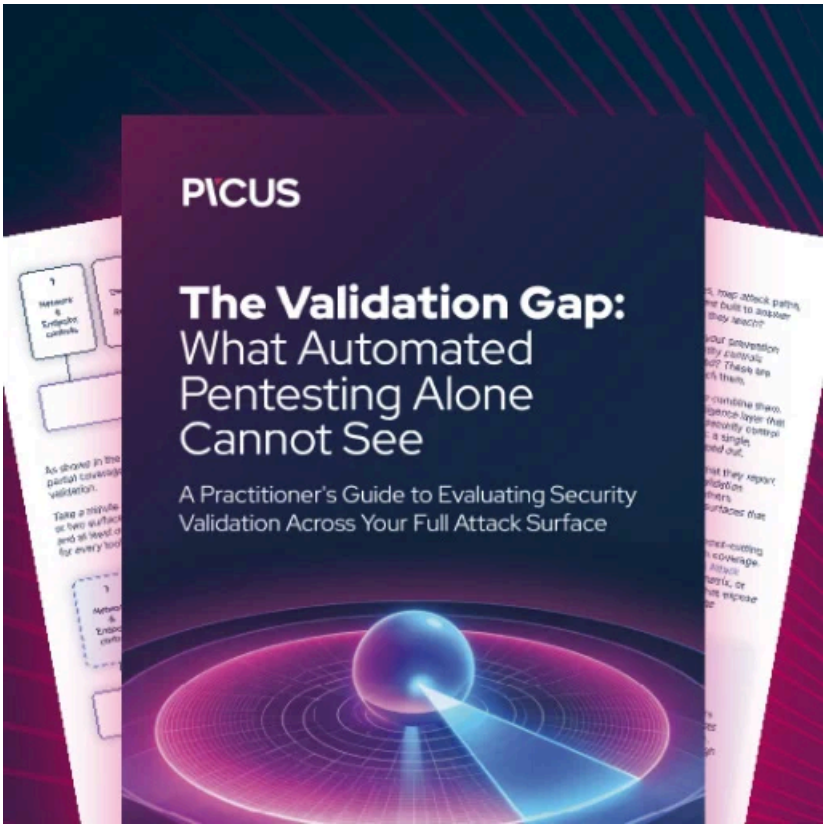
This vulnerability was used to download and steal substantial technical data from the company's internal server.




**Kimsuky attack overview**

*Korean police*

The Korean police recommends both defense companies and their subcontractors to improve network security segmentation, periodic password resets, setting up two-factor authentication on all critical accounts, and blocking foreign IP accesses.




## Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: https://www.bleepingcomputer.com/news/security/dprk-hacking-groups-breach-south-korean-defense-contractors/