NIS Press Release - cyber attacks targeting domestic semiconductor equipment companies

- News/Information
- Notifications/News

press release

The National Intelligence Service discovered that North Korea was focusing on cyber attacks targeting domestic semiconductor equipment companies from the second half of last year until recently, and urged related industries to be careful.

North Korean hacking organizations targeted companies whose servers were connected to the Internet and exposed vulnerabilities. The company's business servers, which are used to manage documents and other data, were targeted by hackers.

They mainly used the 'LotL (Living off the Land)' technique, which minimizes the use of 'malicious code' and attacks using normal programs installed within the server. This method is not easily visible to attackers, so it is not easy to detect even with security tools.

In December last year, Company A, and in February this year, Company B had their configuration management server and security policy server hacked, respectively, and product design drawings and facility site photos were stolen.

In relation to this hacking trend, the National Intelligence Service believes that North Korea may have begun preparing to produce its own semiconductors due to difficulties in procuring semiconductors due to sanctions against North Korea and increased demand due to the development of weapons such as satellites and missiles.

Accordingly, the National Intelligence Service notified the hacking victim of the facts and supported the establishment of security measures. In addition, to prevent further damage, threat information was provided to major domestic semiconductor companies to conduct their own security checks.

An official from the National Intelligence Service urged, “Security updates and access control must be implemented for Internet-exposed servers, and account management must be thorough, including regular administrator authentication reinforcement.”

Meanwhile, the National Cyber Security Center is posting a variety of content containing ways to prevent hacking damage, such as webtoons, videos, and card news, in the cyber security corner of the data room on its website (www.ncsc.go.kr).