North Korean hackers linked to defense sector supply-chain attack

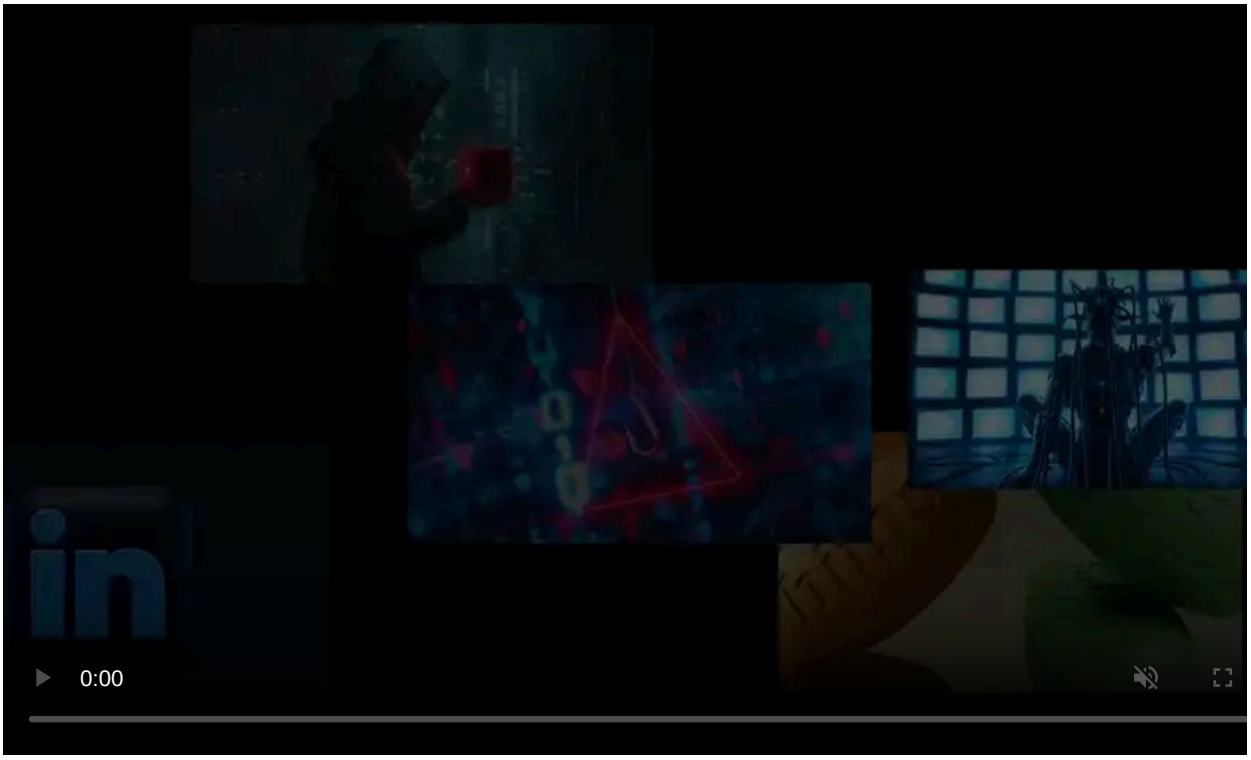
By Bill Toulas

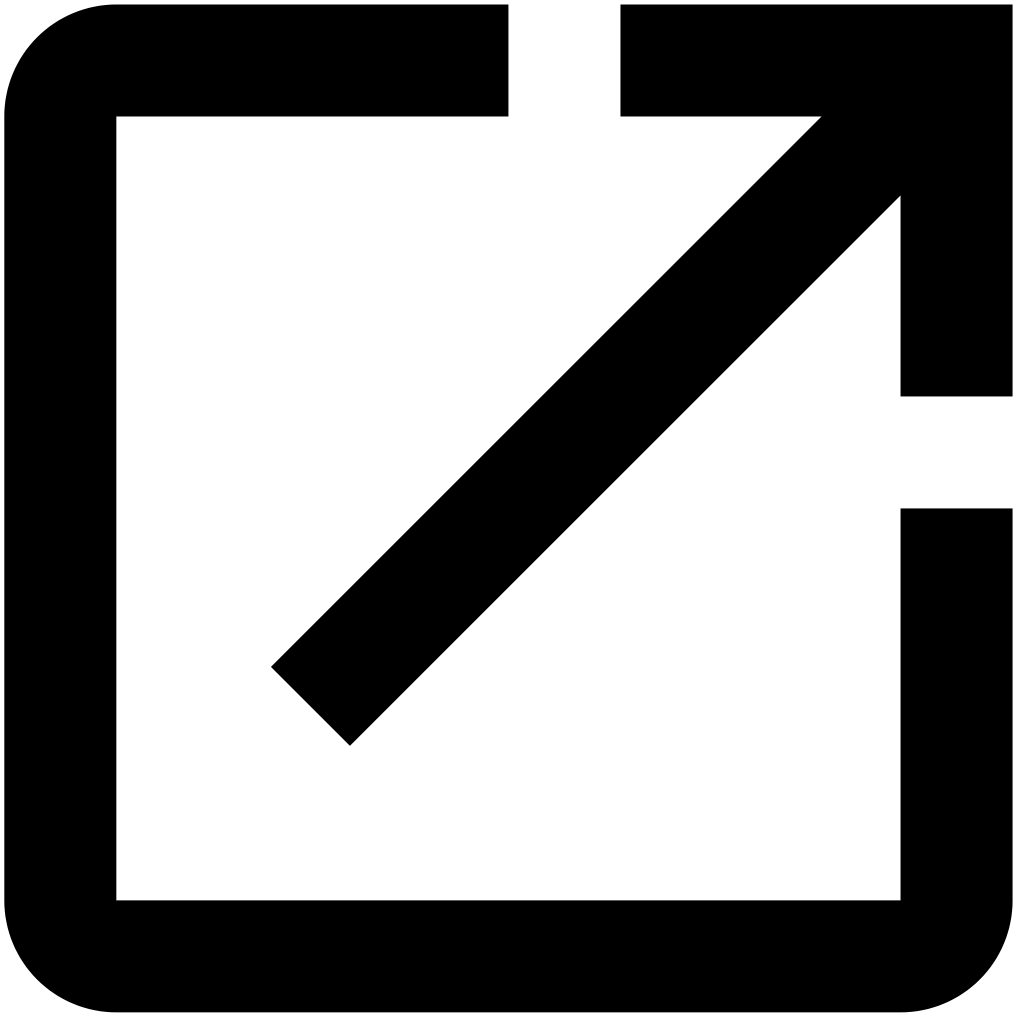
Published: 2024-02-19 · Archived: 2026-04-05 16:01:53 UTC

In an advisory today Germany's federal intelligence agency (BfV) and South Korea's National Intelligence Service (NIS) warn of an ongoing cyber-espionage operation targeting the global defense sector on behalf of the North Korean government.

The attacks aim to steal advanced military technology information and help North Korea modernize conventional arms as well as develop new military capabilities.

Today's joint cybersecurity advisory (also available in Korean and German) highlights two cases attributed to North Korean actors, one of them the Lazarus group, to provide the tactics, techniques, and procedures (TTPs) used by the attackers.


0:00



Visit Advertiser websiteGO TO PAGE

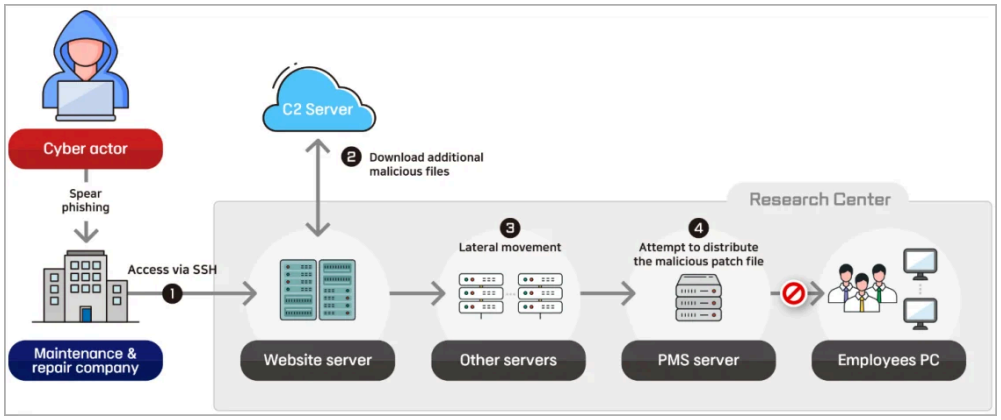
Supply-chain attack

According to the advisory, the first case refers to an incident that occurred at the end of 2022, when "a North Korean cyber actor intruded systems of a research center for maritime and shipping technologies" and "executed a supply-chain attack" by compromising the firm that managed the target organization's web server maintenance operations

The intruder followed an attack chain that included stealing SSH credentials, abusing legitimate tools, moving laterally on the network, and trying to remain hidden on the infrastructure.

Specifically, the advisory lists the following attack steps:

1. Breached the web server maintenance company, stole SSH credentials, and accessed the research center's Linux webserver.
2. Downloaded malicious files (tunneling tool, Base64 Python script) using legitimate tools like curl, fetched from the command and control (C2) servers.
3. Conducted lateral movement: established SSH to other servers, used tcpdump for packet collection, and stole employee account credentials.
4. Impersonated a security manager using stolen account info and attempted to distribute a malicious patch file via PMS, but was blocked by the genuine manager.
5. Persisted by exploiting the website's file-upload vulnerability, uploaded a web shell, and sent spear-phishing emails.



Supply chain attack overview *(verfassungsschutz.de)*

By first compromising the IT services provider, the North Korean threat actor was able to infiltrate an organization that maintains a good security posture, taking advantage of the relationship between the two to carry out covert attacks in small, careful steps.

The bulletin suggests several security measures against these attacks, including limiting IT service providers' access to systems necessary for remote maintenance, closely monitoring access logs to detect unauthorized access events, using multi-factor authentication (MFA) on all accounts, and adopting strict user authentication policies for the patch management system (PMS).

Social engineering

The second example shows that Lazarus group's "Operation Dream Job," a tactic the North Korean actors are known to use against employees of cryptocurrency firms and software developers, was also used against the defense sector.

ESET highlighted a similar incident in September 2023, where Lazarus targeted an employee of an aerospace company in Spain to infect systems with the 'LightlessCan' backdoor.

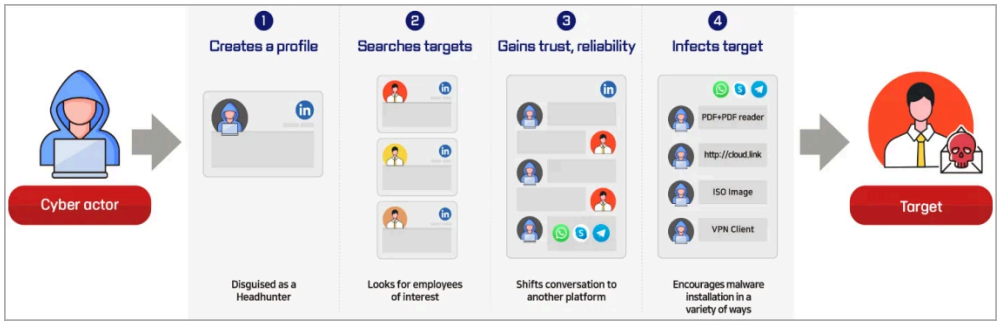
The security bulletin highlights a case where Lazarus creates an account on an online job portal using fake or stolen personal data of an existing person and curates it over time so that it is networked with the right people for the social engineering goals in the campaign.

Next, the threat actor uses that account to approach people working for defense organizations and connects with them to start a conversation in English, slowly building a connection over multiple days, weeks, or even months.

After gaining the victim's trust, the threat actor offers them a job and suggests an external communication channel where it can share a malicious PDF file that is described as a document with details about the offer.

This file is typically a first-stage launcher that drops malware on the target's computer, which Lazarus then uses as an initial foothold to move within the corporate network.

In some cases, Lazarus sends a ZIP file that contains a malicious VPN client, which they use to access the victim's employer network.



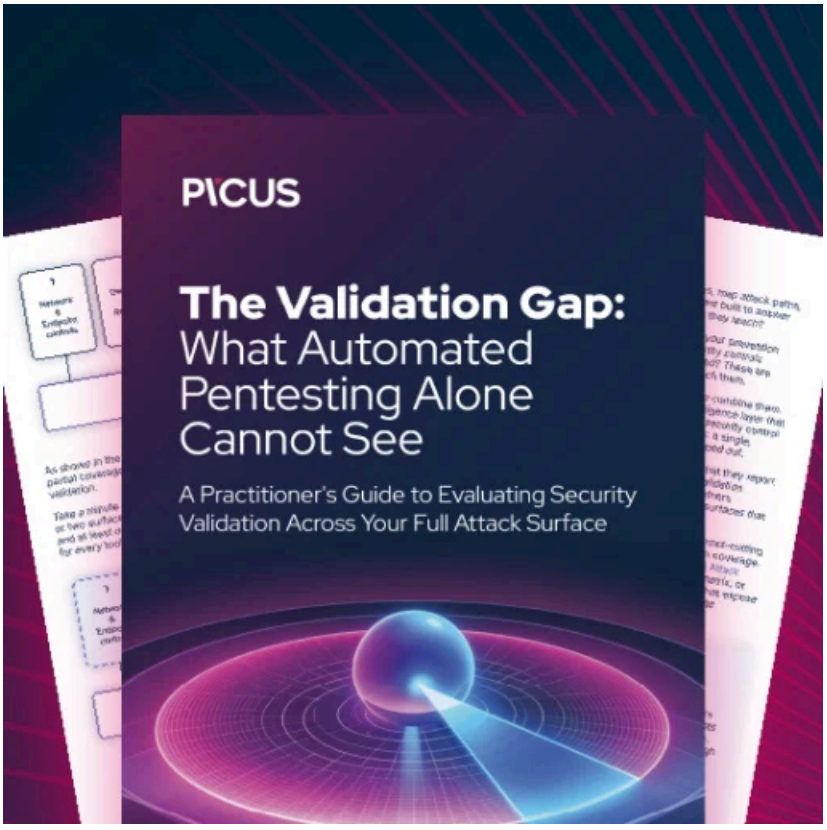
Overview of Lazarus' social engineering attack *(verfassungsschutz.de)*

While these are known tactics, they can still be successful unless organizations educate their employees about the latest trends in cyberattacks.

Adopting the principle of least privilege and restricting employee access only to the systems they need should be the start for a good security posture.

Adding strong authentication mechanisms and procedures for the patch management system and maintaining audit logs that include user access should improve the security stance.

For social engineering attacks, the two agencies recommend training employees on common tactics.



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/north-korean-hackers-linked-to-defense-sector-supply-chain-attack/