North Korean hackers exploit VPN update flaw to install malware

By Bill Toulas

Published: 2024-08-05 · Archived: 2026-04-05 12:35:57 UTC

South Korea's National Cyber Security Center (NCSC) warns that state-backed DPRK hackers hijacked flaws in a VPN's software update to deploy malware and breach networks.

The advisory connects this activity with a nationwide industrial factories modernization project Kim Jong-un, the North Korean president, announced in January 2023, believing the hackers are looking to steal trade secrets from South Korea.

The two threat groups implicated in this activity are Kimsuky (APT43) and Andariel (APT45), state-sponsored actors previously linked to the notorious Lazarus Group.


DIE LINKE.
0:00

"The Information Community attributes these hacking activities to the Kimsuky and Andariel hacking organizations under the North Korean Reconnaissance General Bureau, noting the unprecedented nature of both organizations targeting the same sector simultaneously for specific policy objectives," warns the NCSC.

Trojanized updates and installers

In the first case highlighted in the advisory, dated January 2024, Kimsuky compromised the website of a South Korean construction trade organization to disseminate malware to visitors.

According to a February report by ASEC, when employees attempted to log into the organization's website, they were prompted to install required security software called "NX_PRNMAN" or "TrustPKI."

These trojanized installers were digitally signed with a valid certificate from Korean defense company "D2Innovation," effectively bypassing antivirus checks.

When the trojanized software was installed, the malware was also deployed to capture screenshots, steal data stored in browsers (credentials, cookies, bookmarks, history), and steal GPKI certificates, SSH keys, Sticky Notes, and FileZilla data.

This campaign infected the systems of South Korean construction companies, public institutions, and local governments.

Kimsuky Supply Chain Attack Overview
Source: NCSC

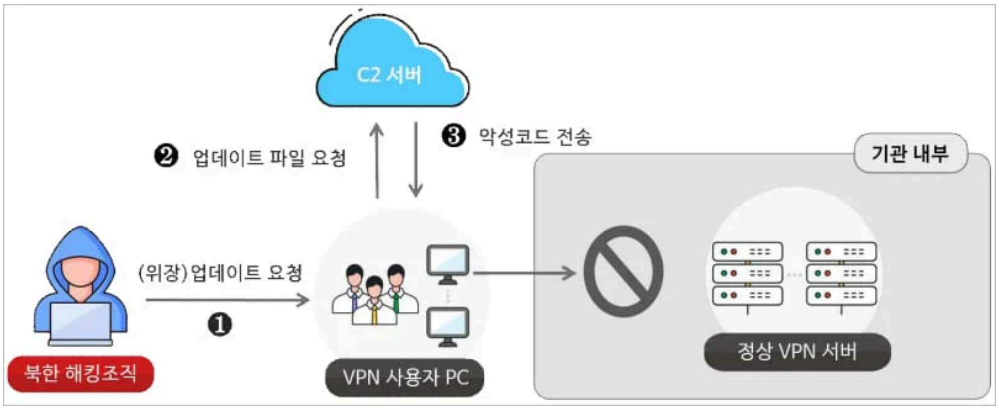
The second case occurred in April 2024, when the NCSC says the Andariel threat actors exploited a vulnerability in a domestic VPN software's communication protocol to push out fake software updates that install the DoraRAT malware.

"In April 2024, the Andariel hacking group exploited vulnerabilities in domestic security software (VPN and server security) to replace update files with malware, distributing remote control malware named "DoraRAT" to construction and machinery companies," explains a machine-translated version of the NCSC advisory.

The NCSC says the vulnerability allowed the threat actors to spoof packets to users' PCs, which misidentified them as legitimate server updates, allowing the malicious versions to be installed.

DoraRAT is a lightweight remote access trojan (RAT) with minimal functionality that allows it to operate more stealthily.

The variant observed in the particular attack was configured for stealing large files, such as machinery and equipment design documents, and exfiltrating them to the attacker's command and control server.



Andariel supply chain attack overview

Source: NCSC

The NCSC says operators of websites at risk of being targeted by state-sponsored hackers should request security inspections from Korea's Internet & Security Agency (KISA).

Additionally, it is recommended that strict software distribution approval policies be implemented and administrator authentication be required for the final distribution stage.

Other generic advice includes timely software and OS updates, ongoing employee security training, and monitoring government cybersecurity advisories to identify and stop emerging threats quickly.

In similar activity, a Chinese hacking group breached an ISP to poison DNS entries so automatic software updates for legitimate software installed malware instead.

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