Kimsuky-linked hackers use similar tactics to attack Russia and South Korea, researchers say

By Daryna Antoniuk

Published: 2024-09-09 · Archived: 2026-04-05 14:49:59 UTC

The threat actor known as Konni, which has been previously linked to the North Korean state-sponsored group Kimsuky, is intensifying its attacks on South Korea and Russia, according to a recent report.

The group employs similar tactics, techniques and procedures in its attacks on both Moscow and Seoul, said researchers at the South Korean cybersecurity company Genians. The primary goal of these attacks is cyber espionage.

Since at least 2021, Konni has targeted the Russian Ministry of Foreign Affairs, the Russian Embassy in Indonesia and several unnamed South Korean enterprises, including a tax law firm.

For example, in January 2022, Konni targeted Russian embassy diplomats during the winter holidays with emails carrying New Year greetings in an attempt to infect them with malware. According to Genians, the group's activity dates back to 2014 and continues to this day.

The suspected North Korean hackers use phishing emails to gain initial access to targeted systems, often using topics such as taxes, scholarships and finance as lures in the malicious emails. Konni's custom remote access trojan grants the attackers full control over the infected systems.

In attacks on both Russia and South Korea, the group uses similar techniques to connect infected devices to hacker-controlled command servers (C2). In both cases, malicious modules are installed on victims' devices through executable files, and the process of connecting to the C2 server is carried out through internal commands, according to Genians.

"Threat actors have been using similar patterns and attack scenarios for years," the researchers said. "However, they are also combining anomalous attack tactics to increase their success rate."

Researchers noted that paying attention to the similarities between the group's attacks in different countries could help security specialists better protect their entities and more accurately attribute the attacks.

Daryna Antoniuk

is a reporter for Recorded Future News based in Ukraine. She writes about cybersecurity startups, cyberattacks in Eastern Europe and the state of the cyberwar between Ukraine and Russia. She previously was a tech reporter for Forbes Ukraine. Her work has also been published at Sifted, The Kyiv Independent and The Kyiv Post.
