Confirmed: North Korean malware found on Indian nuclear plant's network

By Written by Catalin Cimpanu, ContributorContributor Oct. 30, 2019 at 5:06 a.m. PT

Archived: 2026-04-05 14:01:45 UTC

Image via indiawaterportal.org

The network of one of India's nuclear power plants was infected with malware created by North Korea's state-sponsored hackers, the Nuclear Power Corporation of India Ltd (NPCIL) confirmed today.

News that the Kudankulam Nuclear Power Plant (KNPP) might have been infected with a dangerous strain of malware first surfaced on Twitter on Monday.

Pukhraj Singh, a former security analyst for India's National Technical Research Organization (NTRO), pointed out that a recent VirusTotal upload was actually linked to a malware infection at the KNPP.

The particular malware sample included hardcoded credentials for KNPP's internal network, suggesting the malware was specifically compiled to spread and operate inside the power plant's IT network.

Malware linked to North Korea's Lazarus Group

Several security researchers identified the malware as a version of Dtrack, a backdoor trojan developed by the Lazarus Group, North Korea's elite hacking unit.

Singh's tweet and revelation immediately went viral because just days before, the same power plant had an unexpected shutdown of one of its reactors -- with many users conflating the two unrelated incidents as one.

Initially, KNPP officials denied that they've suffered any malware infection, issuing a statement to describe the tweets as "false information," and that a cyber-attack on the power plant was "not possible."


knpp-statement-1.png
Image: ZDNet

But today, NPCIL, the KNPP's parent company, admitted to the security breach in a separate statement.

"Identification of malware in NPCIL system is correct," the statement started.

NPCIL said the malware only infected its administrative network, but did not reach its critical internal network, the one used to control the power plant's nuclear reactors. NPCIL said the two networks were isolated.

In addition, NPCIL confirmed statements made by Singh on Twitter; that they received notification from CERT India back on September 4, when the malware was first spotted, and that they investigated the matter at the time of the report.

Not actually a big deal

According to an analysis of the Dtrack malware from Russian antivirus maker Kaspersky, this trojan includes features for:

- keylogging,
- retrieving browser history,
- gathering host IP addresses, information about available networks and active connections,
- listing all running processes,
- listing all files on all available disk volumes.

As evident from its features, Dtrack is usually used for reconnaissance purposes and as a dropper for other malware payloads.

Previous Dtrack samples have been usually spotted in politically-motivated cyber-espionage operations, and in attacks on banks -- with a custom version of Dtrack, named AMTDtrack also being discovered last month.

Historically, the Lazarus Group or any other North Korean hacker group, have rarely gone after targets in the energy and industrial sector. When they did, they went after proprietary intellectual property, rather than sabotage.

Most of North Korea's offensive hacking efforts have been focused on attaining insight into diplomatic relations, tracking former North Korean citizens who fled the country, or hacking banks and cryptocurrency exchanges to gather funds for the Pyongyang regime to raise funds for its weapons and missile programs.

The KNPP incident looks more like an accidental infection, rather than a well-planned operation. This specifically seems to be the case, since Kaspersky reported last month that the Lazarus Group had been spotted spreading Dtrack and AMDtrack versions across India, targeting its financial sector.

Article updated shortly after publication to include link to McAfee research on previous North Korean campaigns targeting the energy and industrial sector.

North Korea's history of bold cyber attacks

Security

Source: https://www.zdnet.com/article/confirmed-north-korean-malware-found-on-indian-nuclear-plants-network/