Unverified reports circulated this week that the power plant – the largest operating nuclear power plant in India – had suffered a cyber attack. The reports claimed that a version of the 'DTrack RAT' virus had infected the plant's administrative systems.

According to Kaspersky, which named the virus, DTrack has been used in cyberattacks against financial bodies in India as a tool for aggressively extracting data from infected systems. The malware came to prominence in September this year after being blamed for an espionage attack on Indian ATMs.

The malware appears to be connected to the Lazarus group, which has been identified by the US Department of Justice as a North Korean-backed cyber-crime organisation. Some organisations have linked the Lazarus group to the WannaCry ransomware attacks which briefly rocked the NHS and other major institutions around the world in May 2017.

What New Delhi thinks?

Image: Kudankulam Nuclear Plant

Authorities from the Nuclear Power Corporation of India Limited (NPCIL) have admitted that malware, believed to originate from the Lazarus Group, infected the administrative

network of the Kudankulam Nuclear Power Plant.

Initial reports about possible problems with the Kudankulam Nuclear Power Plant (KKNPP) surfaced a couple of days ago when a researcher who used to work for India's National Technical Research Organization (NTRO) made the connection by using published results from VirusTotal. Now, the NPCIL has admitted that intruders had access to an administrative network.

Pukhraj Singh, the researcher who discovered the intrusion, referred to the event as casus belli, a Latin term used to describe an act of war. Talking with Ars Technica, Singh explained that he called the event an act of war because of a second target, which he also reported to the government, but didn't want name publicly.

"Indication of malware in the NPCIL system is correct," said NPCIL Associate Director A. K. Nema in a communique. "The matter was conveyed by CERT-in when it was noticed by them on September 4, 2019. The matter was immediately investigated by DAE specialists."

"The investigation revealed that the infected PC belonged to a user who was connected to an Internet-connected network used for administrative purposes. This is isolated from the critical internal network. The networks are being continuously monitored."

The fact that the intrusion was found accidentally could mean the hackers didn't want to make their presence known. It's unclear whether any information was stolen, and there's no indication of what the second target might be.

The views and opinions expressed in this article are those of the author and do not necessarily reflect the views of The Kootneeti Team