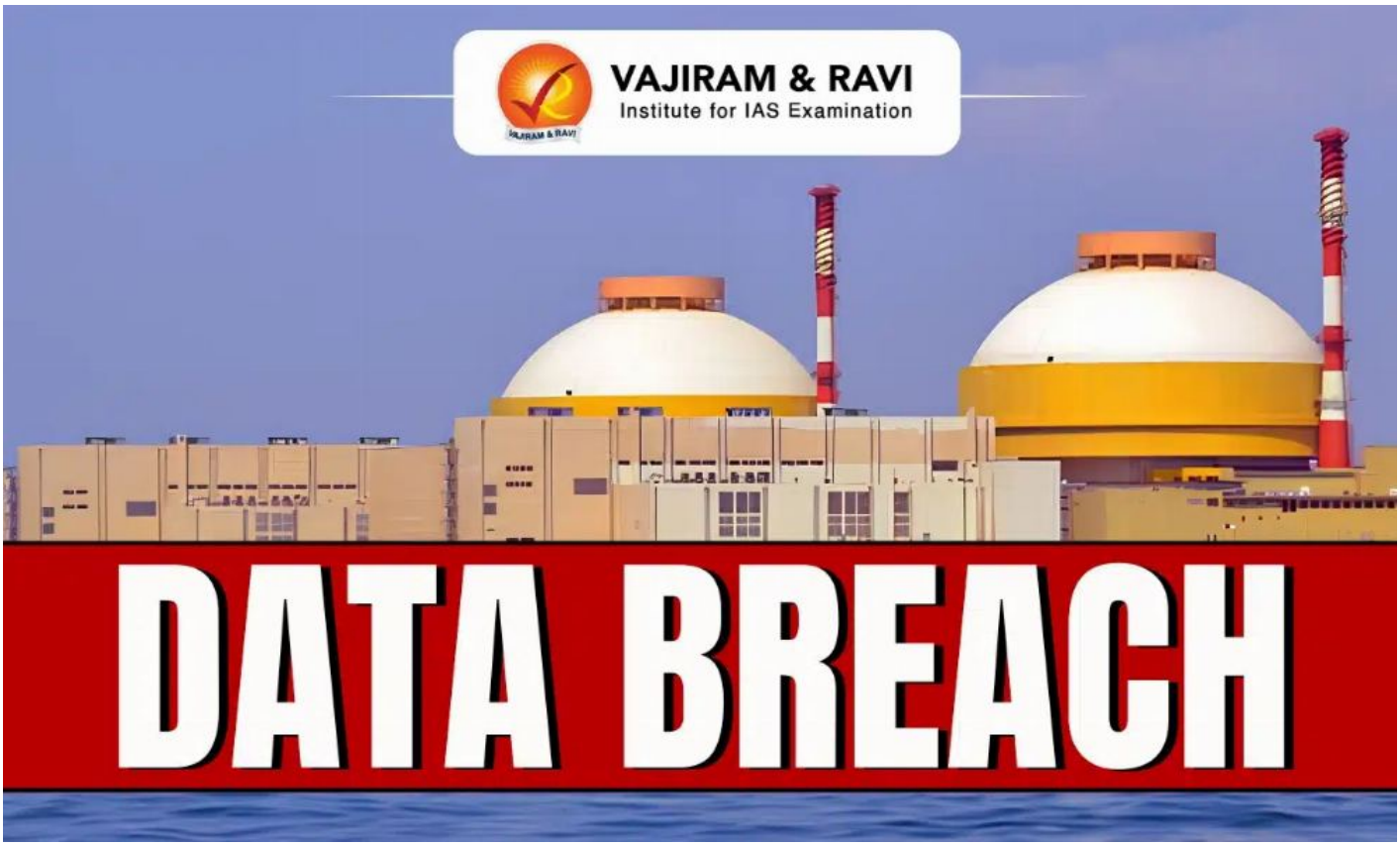
Kudankulam Nuclear Power Plant Data Breach – Explained

July 19, 2026 • vajiramandravi.com



Data Breach Latest News

- A ransomware group named World Leaks has allegedly leaked documents related to the Kudankulam Nuclear Power Plant (KKNPP), reigniting concerns over cybersecurity vulnerabilities in India's critical infrastructure.

Background of the Data Breach

- The **Kudankulam Nuclear Power Plant** **(KKNPP)**, located in the **Tirunelveli district of Tamil Nadu**, is India's largest nuclear power generation facility and a flagship Indo-Russian civil nuclear project.
- Recently, a ransomware group known as **World Leaks** allegedly published several internal documents relating to the plant on the dark web.
- The leaked material reportedly included:
    - Engineering drawings
    - Inspection records

    - Minutes of meetings
    - Technical reports
    - Official correspondence
- Responding to the reports, the **Nuclear Power Corporation of India Limited (NPCIL)** clarified that the leaked documents pertained only to non-critical facilities located outside the “reactor island” and did not compromise nuclear safety or reactor operations.
- The reactor island is the highly secured section of a nuclear power plant that houses the nuclear reactor and associated safety systems.
- Although the NPCIL maintained that there was no threat to reactor safety, the incident has raised concerns regarding the cybersecurity preparedness of India’s strategic infrastructure, particularly at a time when the government is seeking greater private sector participation in the civil nuclear sector.
- The breach has also revived memories of the 2019 cyberattack on the Kudankulam Nuclear Power Plant, which remains one of the most significant cybersecurity incidents involving India’s nuclear establishment.

The 2019 Kudankulam Cyberattack

- The 2019 incident came to light after malware-related data associated with the plant appeared on **VirusTotal**, an online malware scanning platform.
- Subsequent investigations by cybersecurity agencies attributed the intrusion to **DTrack malware**, which has been linked to the **Lazarus Group**, a North Korea-backed hacking organisation known for conducting cyber espionage and financial cyberattacks.
- According to cybersecurity experts, DTrack belonged to the same malware family that was responsible for the 2016 cyberattack on an Indian private bank’s ATM network, which resulted in the replacement of nearly three million debit and credit cards.
- The malware reportedly targeted the domain controller of Kudankulam’s administrative network.
- A domain controller is the central server responsible for authenticating users and managing access across a computer network. By compromising this server, attackers could potentially obtain sensitive credentials such as usernames and passwords.
- Cybersecurity researchers further suggested that the attackers were interested in obtaining information related to **India’s thorium-based nuclear programme**, an area in which India has invested significant long-term research owing to its abundant thorium reserves.
- According to reports, the attack was initiated through **malware-laced links sent to senior nuclear scientists**, including retired scientists who continued to use official institutional email accounts.
- Once these links were opened on systems connected to the plant’s administrative network, the malware spread across the network.
- Initially, plant officials denied any cyberattack. However, the NPCIL later acknowledged that **CERT-In (Indian Computer Emergency Response Team)** had alerted it about the malware infection in September 2019.
- The organisation clarified that the infected computer belonged to the **internet-connected administrative network**, while the **critical reactor control systems remained unaffected** because they operated on a separate network.

About Air-Gapped Networks

- High-security facilities such as nuclear power plants generally operate using air-gapped networks.
- An air-gapped network is a computer network that is physically isolated from unsecured external networks, including the public internet. This physical separation significantly reduces the risk of remote cyber intrusions into critical operational systems.
- Typically, nuclear facilities maintain two separate networks:
    - **Operational Technology (OT) Network:** Controls reactors, turbines, and other critical plant operations.
    - **Information Technology (IT) Network:** Supports administrative functions such as communication, documentation, procurement, and personnel management.
- While air-gapping provides an important layer of protection, it is not completely foolproof.
- Malware can still enter through infected USB devices, compromised maintenance equipment, insider threats, or phishing attacks targeting users connected to the administrative network.
- Globally, even air-gapped systems have been compromised in incidents such as the Stuxnet attack on Iran's nuclear programme, the Davis-Besse Nuclear Power Station breach (USA), and cyber intrusions into classified military networks.

Significance of Cybersecurity for Nuclear Infrastructure

- Nuclear facilities form part of a country's **Critical Information Infrastructure (CII)**, whose disruption could have severe implications for:
    - National security
    - Public safety
    - Energy security
    - Environmental protection
    - Economic stability
- Unlike conventional cyberattacks that primarily target financial losses or data theft, attacks on nuclear infrastructure may attempt to:
    - Steal sensitive scientific and engineering information
    - Conduct strategic espionage
    - Disrupt operational systems
    - Undermine public confidence in nuclear safety
    - Target critical national infrastructure during geopolitical conflicts
- Given the increasing sophistication of ransomware groups and state-sponsored cyber actors, securing both operational and administrative networks has become an essential component of national security.

Measures Taken to Strengthen Cybersecurity

- India has undertaken several initiatives to strengthen the cybersecurity of critical infrastructure, including:
- **Indian Computer Emergency Response Team (CERT-In):** The national agency responsible for responding to cybersecurity incidents.
- **National Critical Information Infrastructure Protection Centre (NCIIPC):** Established under the Information Technology Act, 2000, to protect critical information infrastructure across sectors such as power,

banking, telecommunications, transport, and strategic facilities.

- **National Cyber Security Policy, 2013:** Provides the framework for securing cyberspace and strengthening cyber resilience.
- Regular cybersecurity audits, penetration testing, and network monitoring by strategic organisations.
- Adoption of **air-gapped operational networks** and enhanced access control mechanisms in sensitive installations.

Source: IE | TH
