CYDEF THREAT RESEARCH

Kudankulam Nuclear Power Plant Cyber Attack
September 2019

Overview

In early September 2019, the Kudankulam Nuclear Power Plant in Tamil Nadu in India suffered a cyber intrusion. On September 3, a local security expert and former member of the Indian signals intelligence agency received a tip that there had been a malware attack and informed the Indian CERT on September 4. The attack was investigated by the Indian Department of Atomic Energy which concluded only one administrative machine was affected. However, on October 27, the local security expert published on Twitter that there had been a domain controller-level compromise and that extremely mission-critical systems targets hit. This led to a public statement by the Nuclear Power Corporation of India Limited (NPCIL) on October 29 that “any cyber-attack on the Nuclear Power Plant Control System is not possible.” However, on the next day, they had to walk back the statement and confirm that a cyber intrusion had taken place in early September.

The exact scope of the acknowledged attack is not specified, so it is not possible to determine if they are referring to the single computer impact on the administrative side or the larger compromise alluded to by the security expert.

The attack was later attributed to the North Korean state-sponsored attack group, Lazarus.

Objective

In this incident, it is not possible to discern the exact motives behind the attack. As the attackers are affiliated with North Korea, which possesses an active nuclear weapons program that is hindered by international sanctions, a likely scenario could be the theft of nuclear expertise. However, the group is also associated with a number of disruptive attacks, notably the Dark Seoul attack against South Korean broadcaster and financial sector, the Sony Pictures attack and the WannaCry ransomware.

Tools, Techniques and Procedures (TTPs)

Because the technical details of the attack are not available, it is not possible to establish the TTPs used in this attack. However, Dragos tracks the cluster of activity linked with the attack group that perpetrated this attack as Wassonite. They report the group as relying mostly on the Dtrack malware, which is a typical espionage backdoor according to Kaspersky, as their initial point of presence of the victim network. Then, the attack group relies on publicly available hacker tools to perform other post-exploitation tasks. Notably, they make heavy use of Mimikatz to expand their access.

The Dragos information stipulates that the group focuses on ICS-related targets in South Korean, India and Japan, but that they typically focus on IT targets in those organizations and have no ICS-specific attack toolkits. However, as seen in the 2015 Ukraine black-out attack, this does not preclude them from compromising key elements such as operator workstations.

Analysis

Because publicly available information on the incident is so murky, it is difficult to perform a deep analysis of the incident. The sequence of events supports multiple hypotheses. For example, it may be possible that the attack only compromised a machine on the administrative side of the power plant and the local security analyst exaggerated the impact on Twitter. It is also possible that the compromise was very severe and the NPCIL is lying to protect its image or public confidence. It could also be possible that the incident was severe, but the cyber investigation was botched and only the initial foothold of the attacker was found after they had successfully expanded their access and so, in their perspective, everyone is telling the version of the truth they could observe, even if that was not the reality on the ground.

However, the Bulletin of Atomic Scientists published a report on the lessons learned from the Indian nuclear power plant attack. In this report, they focus on the management of the incident by the NPCIL. In particular, they point out the blind faith the authorities had in the “air-gap” between the critical plant operation systems and the IT network and the general lax attitude to cyber threats. The report points out multiple incidents in which cyber attacks have crossed air-gaps as proof that air-gaps do not provide the reliable defense mechanism that many believe. In fact, they argue that the blind faith in air-gapping engenders a complacency toward cyber threats that is very dangerous. Famously, the belief that the Titanic was unsinkable emboldened the captain to pursue a risky course of action which ultimately sank the ship.

Key Lessons Learned

- Relying solely on air-gap does not provide sufficient protection against cyber incidents;
- Air-gaps need to be complemented with additional layers of defenses.

Our mailing address is:
1505 Laperriere Ave #308, Ottawa, ON K1Z 7T0