WATER & SEWERAGE

Sector Overview

In 2000, a cyber-attack against water and sewerage infrastructure in Maroochydore, Queensland, became the world's first publicly known example of a successful hack against a SCADA infrastructure system to cause significant damage. For cybersecurity professionals worldwide, this Critical Infrastructure (CI) attack remained the most studied malicious cyber incident until the world-famous Stuxnet cyber-attack in 2010; extensive analyses by MIT and MITRE are a testament to this.

Today, water and sewerage systems remain vulnerable to cyber-physical attacks (CPAs) that can disrupt operational functionality and compromise access to sensitive operational and/or customer data. Cyber-attacks against such infrastructure may even result in structural/mechanical damage to the water infrastructure itself, potentially degrade water quality by altering treatment processes or silencing pollution alerts by interfering with water quality sensors.

With a population of 26 million people spread across an expansive continent, it is a testament to Australia's infrastructure investment that 94% of Australians have access to a mains water supply. Adopting new technology to manage geographically dispersed water infrastructure has resulted in significant operational and economic benefits; however, internet-facing control systems and sensors give rise to an array of unique cyber threats and potential exploitation by malicious cyber threat actors.

The water and sewerage sector faces a significant concentration risk in terms of supply, with 7% (22) of the roughly 300 water and sewerage entities servicing 70% of the national population. Adopting a collective defence approach, informed by cyber threat intelligence sharing to protect these critical water assets, is vital in a country that is one of the driest on earth. The converse of this challenge is the tail end of the spectrum, where the 200 smallest water utilities serve just 13% of the national population and lack the resources and capabilities to address cyber threats independently.

Australia spends more than $6 billion annually on water and wastewater treatment services and endured one of the worst droughts of the last 100 years in 2019. Ensuring the continued availability of water and water treatment is a critical issue, with the Australian government recently establishing the 10-year/USD$2.5 billion National Water Grid Fund.

A cyber-attack against water infrastructure has the potential to affect public health and safety, cause expensive systemic damage, and result in personal and commercial data being stolen. The sector is vulnerable to numerous cyber-attack Tactics, Techniques, and Procedures (TTPs) employed by Threat Actors both locally and abroad who seek to compromise IT/OT networks, systems, and devices.

A subset of the common TTPs worth noting for the water and sewerage sector are as follows:

- Spear phishing personnel to deliver malicious payloads, including ransomware [T1556];
- The exploitation of internet-connected services and applications that enable remote access to water and sewerage networks [T1210];
- The exploitation of unsupported or outdated operating systems and software [T1190].

Exploiting outdated operating systems and software is particularly challenging for the water and sewerage sector as already limited resources are prioritised towards physical infrastructure upgrades instead of IT/OT modernisation.

Most water and sewerage entities won't have the capability to share 'machine to machine' intelligence so an industry partner is needed as the enabler/facilitator for cyber threat intelligence (CTI) and collective defence via other means. By taking on the role of the trusted advisor/facilitator for the intelligence exchange, an industry organisation would ensure the overall quality of information flowing through its systems and out to the CI members.

'Forewarned is Forearmed', and by joining a trusted cyber community of Critical Infrastructure owners and operators responsible for protecting their water and sewerage assets, you can join the movement to share contextual intelligence and proactively approach cyber defence. Cyber threat activity shared into the CI-ISAC ecosystem by one member has the potential to help others across the sector and the broader CI community stop similar attacks before they impact operations.

CI-ISAC, as a not-for-profit, member driven organisation, with a mission to serve its members and in turn their customers by building a trusted community and leveraging the best technology in its intelligence platform, and drawing on resources and resilience through its industry peer-to-peer network to anticipate, mitigate, and respond to cyber threats.

More information on CI-ISACs sovereign intelligence-sharing capability can be found on the official website: https://www.ci-isac.com.au , or by emailing info@ci-isac.com.au.

Published: 31st January 2023