Australian Electricity Provider ‘CS Energy’ Hit by Ransomware

By Eduard Kovacs

Published: 2021-12-09 · Archived: 2026-04-05 15:30:38 UTC

Australian electricity provider CS Energy has been hit by a ransomware attack, but the company says electricity generation has not been affected and it has denied claims that the attack was conducted by a state-sponsored threat group.

The attack was discovered on November 27 and the company informed the public about the incident a few days later.

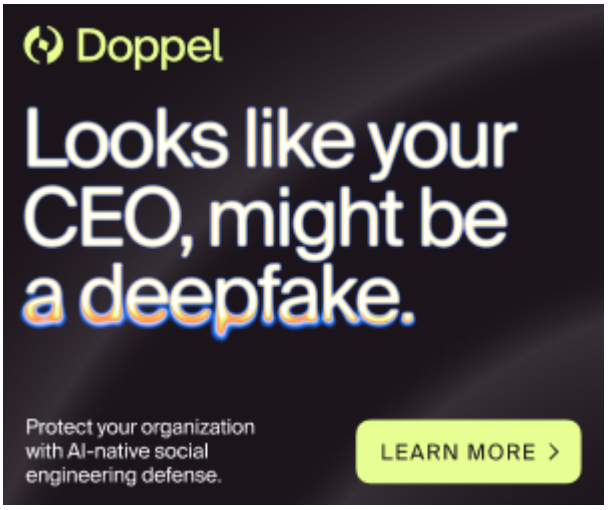
Queensland-based CS Energy, which is owned by the local government, provides electricity to millions of homes, as well as to large commercial and industrial customers in Queensland.

CS Energy said the ransomware compromised devices on its corporate network, which was quickly isolated from other internal networks to prevent the malware from spreading. Safety and operations at its Kogan Creek and Callide power stations were not impacted, nor was power generation and delivery.

The company is working on restoring affected systems and noted that “Australia’s National Electricity Market is designed to ensure there is enough power generation and network capacity to securely meet customer demand, even in the event of unexpected outages of transmission lines and generators.”

Some local news publications claimed — citing sources — that the attack on the energy firm has been linked to Chinese state-sponsored hackers. In response, CS Energy issued a statement on Wednesday to clarify that there was no indication of the attack being “state-based.”

Advertisement. Scroll to continue reading.



In fact, it appears that the attack involved the well-known Conti ransomware, whose operators not only encrypt files on compromised systems, but also steal valuable data in an effort to convince the victim to pay a ransom.

Conti operators run a website where they leak the data of victims that refuse to pay up. CS Energy has been listed on that site since November 27, but the cybercriminals have yet to make public any files associated with the energy company.

CS Energy is not the only electric utility hit by ransomware in recent days. The Delta-Montrose Electric Association (DMEA), a rural electric cooperative that serves more than 34,000 customers in Colorado, suffered significant disruption and damage as a result of a ransomware attack last month, but its power grid was not impacted.

DMEA admitted that the attack resulted in disruption to email, phone and billing systems, as well as the loss of historical data dating back more than 20 years.

Related: Rural Alabama Electric Cooperative Hit by Ransomware Attack

Related: More Threat Groups Target Electric Utilities in North America

Related: Massachusetts Electric Utility Hit by Ransomware

Source: https://www.securityweek.com/australian-electricity-provider-cs-energy-hit-ransomware