Australian govt raises alarm over Conti ransomware attacks

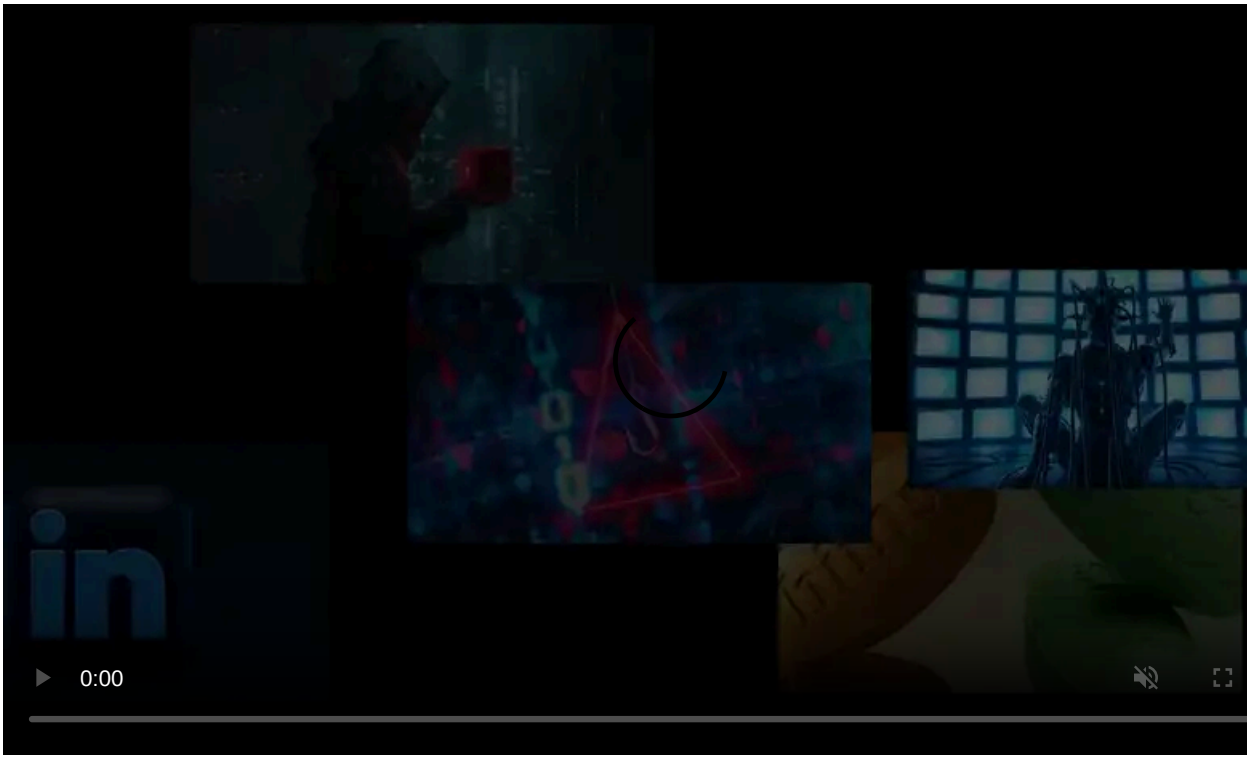
By Sergiu Gatlan

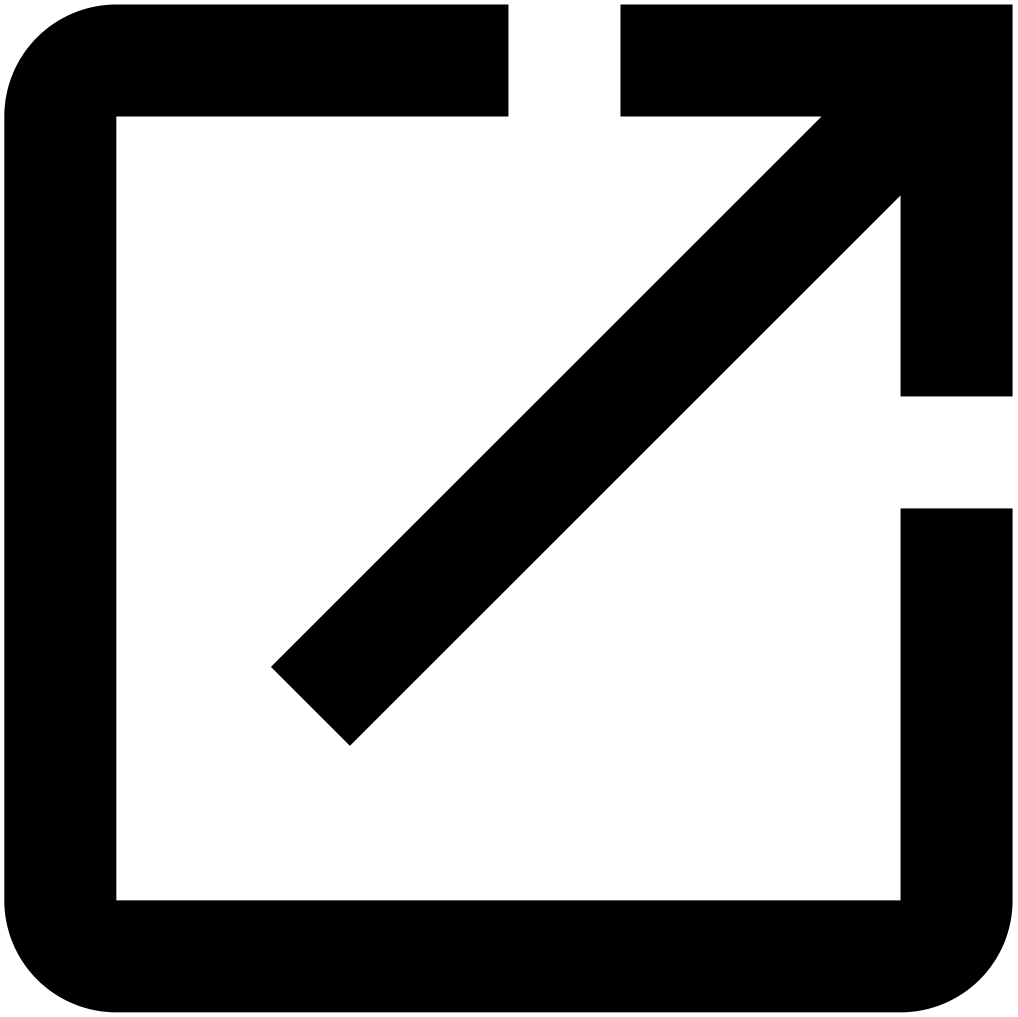
Published: 2021-12-10 · Archived: 2026-04-05 17:33:46 UTC

The Australian Cyber Security Centre (ACSC) says Conti ransomware attacks have targeted multiple Australian organizations from various industry verticals since November.

"The ACSC is aware of multiple instances of Australian organisations that have been impacted by Conti ransomware in November and December 2021.

This activity has happened across multiple sectors. Victims have received demands for ransom payments," Australia's cybersecurity agency warned in a security advisory issued today.


0:00

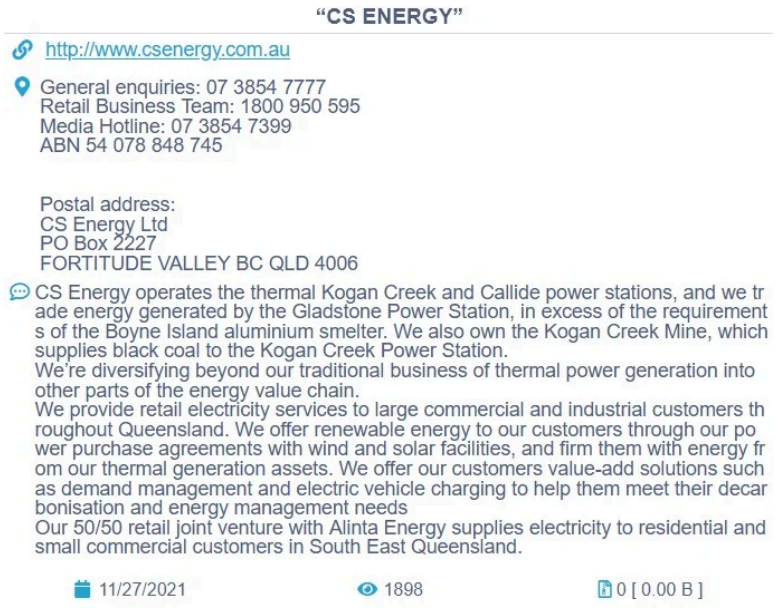


"In addition to the encryption of data and subsequent impact to organisations' ability to operate as usual, victims have had data stolen during incidents published by the ransomware actors, including Personally Identifiable Information (PII)."

The warning follows a November ransomware attack on Australian electricity provider CS Energy's corporate ICT network mistakenly linked by local media to a Chinese-backed hacking group.

However, as CS Energy CEO Andrew Bills revealed, the company didn't "find indication that the cyber incident was a state-based attack."

The Conti ransomware gang claimed the attack on November 27, when the Australian energy provider discovered the intrusion. Conti is yet to leak any files stolen from CS Energy.



CS ENERGY Conti leak page (BleepingComputer)

The ACSC also published a ransomware profile with additional info on the Conti gang, including initial access indicators, targeted sectors, and mitigation measures.

"The threat actors involved in the deployment of the Conti ransomware frequently change attack patterns, and quickly take advantage of newly disclosed vulnerabilities to compromise and operate within networks before network owners are able to apply patches or mitigations," the agency added.

"Conti affiliates have been observed targeting entities in critical sectors, notably including healthcare organisations. In 2021, Conti claimed to have compromised at least 500 organisations worldwide on their TOR site."

The ACSC provides mitigations focused on Conti TTPs (Tactics, Techniques, and Procedures), including:

- enabling multifactor authentication (MFA) to block the use of stolen credentials
- encrypting sensitive data at rest to block sensitive info exfiltration
- segmenting corporate networks and restricting admin privileges to block privilege escalation attempts and lateral movement
- maintaining daily backups to reduce attacks' impact

The agency previously warned of an increase in LockBit 2.0 ransomware attacks targeting Australian orgs starting with July 2021.

Source: https://www.bleepingcomputer.com/news/security/australian-govt-raises-alarm-over-conti-ransomware-attacks/