

Australian govt raises alarm over Conti ransomware attacks

By Sergiu Gatlan

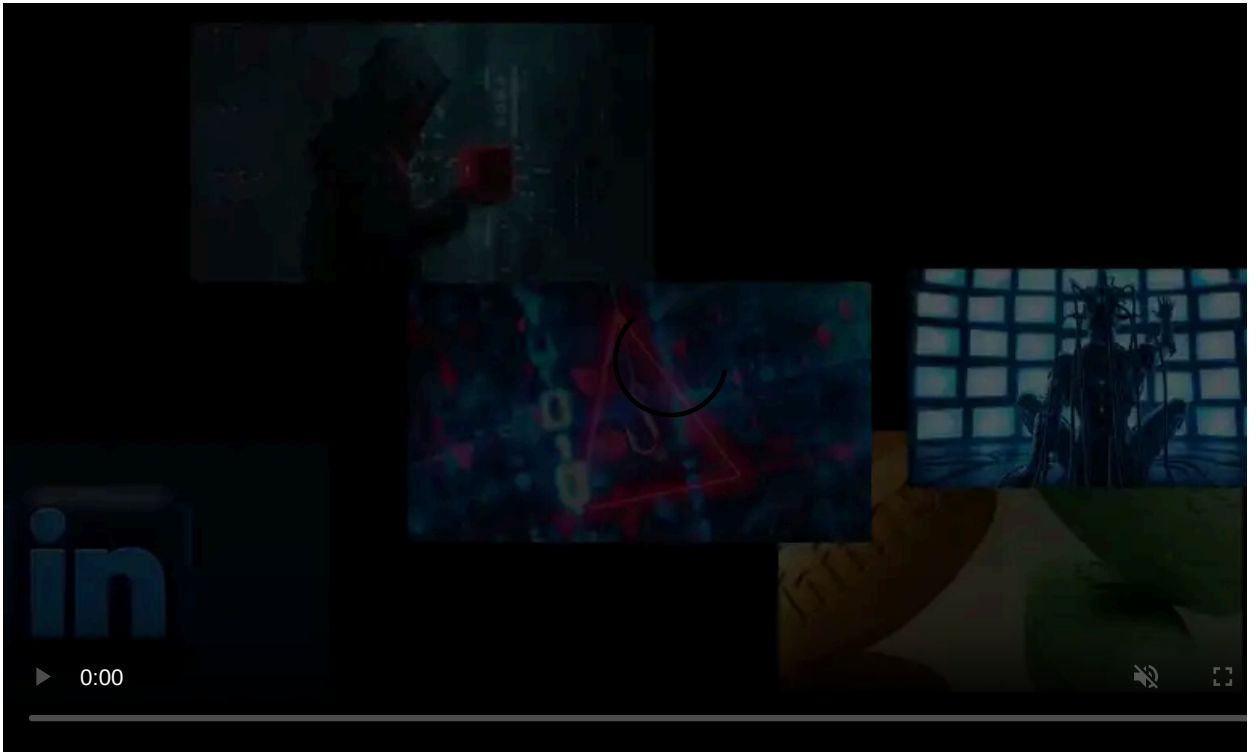
Published: 2021-12-10 · Archived: 2026-04-05 17:33:46 UTC



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.



Visit Advertiser website [GO TO PAGE](#)

"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"

<http://www.csenergy.com.au>

General enquiries: 07 3854 7777
Retail Business Team: 1800 950 595
Media Hotline: 07 3854 7399
ABN 54 078 848 745

Postal address:
CS Energy Ltd
PO Box 2227
FORTITUDE VALLEY BC QLD 4006

CS Energy operates the thermal Kogan Creek and Callide power stations, and we trade energy generated by the Gladstone Power Station, in excess of the requirements of the Boyne Island aluminium smelter. We also own the Kogan Creek Mine, which supplies black coal to the Kogan Creek Power Station. We're diversifying beyond our traditional business of thermal power generation into other parts of the energy value chain. We provide retail electricity services to large commercial and industrial customers throughout Queensland. We offer renewable energy to our customers through our power purchase agreements with wind and solar facilities, and firm them with energy from our thermal generation assets. We offer our customers value-add solutions such as demand management and electric vehicle charging to help them meet their decarbonisation and energy management needs. Our 50/50 retail joint venture with Alinta Energy supplies electricity to residential and small commercial customers in South East Queensland.

11/27/2021 1898 0 [0.00 B]

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.

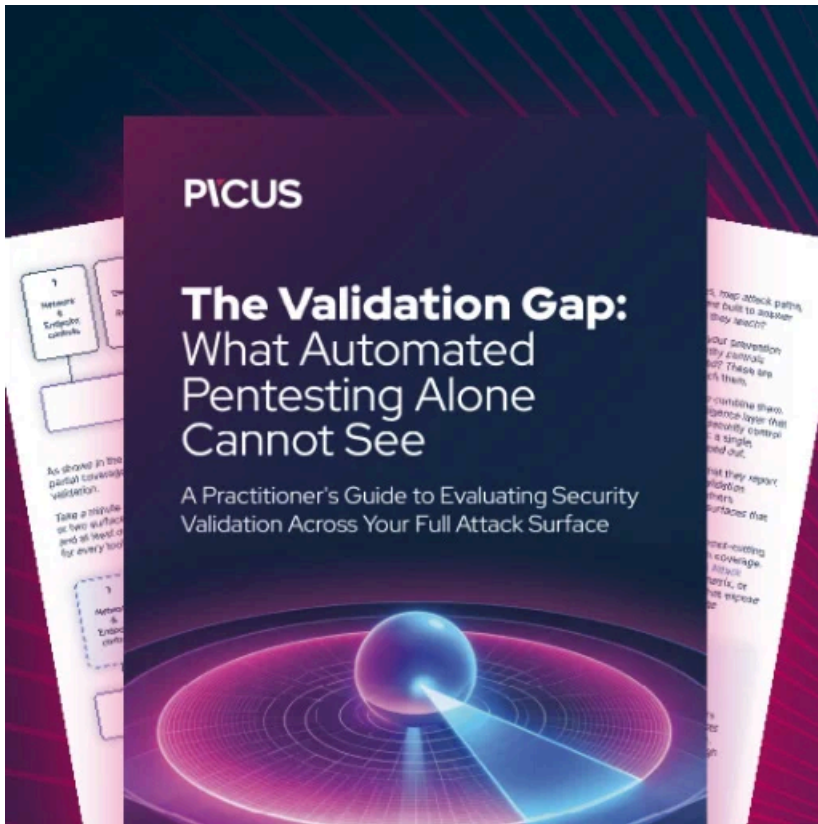
"The threat actors involved in the deployment of the Conti ransomware frequently change attack patterns, and quickly take advantage of newly disclosed vulnerabilities to compromise and operate within networks before network owners are able to apply patches or mitigations," the agency [added](#).

"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.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

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