

Crown Resorts confirms ransom demand after GoAnywhere breach

By Bill Toulas

Published: 2023-03-28 · Archived: 2026-04-05 12:40:16 UTC



Crown Resorts, Australia's largest gambling and entertainment company, has confirmed that it suffered a data breach after its GoAnywhere secure file-sharing server was breached using a zero-day vulnerability.

The Blackstone-owned company has an annual revenue that surpasses \$8 billion and operates complexes in Melbourne, Perth, Sydney, Macau, and London.

This data breach was conducted by the Clop ransomware gang, which has shifted over the past year from encrypting files to performing data extortion attacks.



Visit Advertiser website [GO TO PAGE](#)

In February, the threat actors [claimed to have stolen data from 130 organizations](#) over ten days utilizing a [GoAnywhere zero-day vulnerability](#).

While Crown Resorts confirmed that it is being extorted by Clop, who claims to have stolen data from its networks, it says there is no evidence of the data breach impacting customers.

"We were recently contacted by a ransomware group who claim they have illegally obtained a limited number of Crown files," reads the [firm's statement](#).

"We are investigating the validity of this claim as a matter of priority. We can confirm no customer data has been compromised, and our business operations have not been impacted."

The gambling and entertainment company says they will continue to work with law enforcement to continue the investigation of the security incident and will provide updates if new evidence surfaces.

Crown Resorts is the latest in a long list of victims who have admitted to being impacted by the GoAnywhere breaches, including [CHS](#), [Hatch Bank](#), [Rubrik](#), the [City of Toronto](#), [Hitachi Energy](#), [Procter & Gamble](#), and [Saks Fifth Avenue](#).

Clop is still extorting the victims by threatening to release the data it stole from their networks but has not yet leaked anything on its data leak site.

Headquarters:
8 Whiteman St Shop 88, Southbank, Victoria, 3006, Australia

Phone:
+61 392928824

Website:
www.crownresorts.com.au

Revenue:
\$1.2B

Information:

COMING SOON ...

Clop claiming Crown Resorts as a victim

Source: BleepingComputer

Meanwhile, the vendor of GoAnywhere software, Fortra, is already facing the prospect of a [class action lawsuit](#) in the United States, accused of failing to implement adequate cybersecurity measures to protect the private data stored in its network.

Although Fortra offered the plaintiff, a Hatch Bank customer, one year of free identity monitoring and fraud protection services, the gesture is dismissed as insufficient to mitigate the lifetime risk of personal data exposure.

The Clop ransomware gang has a history of exploiting zero-day flaws to steal data from companies and perform massive extortion waves.

In December 2020, the gang utilized a [zero-day flaw in Accellion FTA](#) to compromise over a hundred firms, including Shell, Kroger, Qualys, and several Universities, demanding \$10,000,000 in extortion demands.



[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/crown-resorts-confirms-ransom-demand-after-goanywhere-breach/>