Qantas discloses cyberattack amid Scattered Spider aviation breaches

By Lawrence Abrams

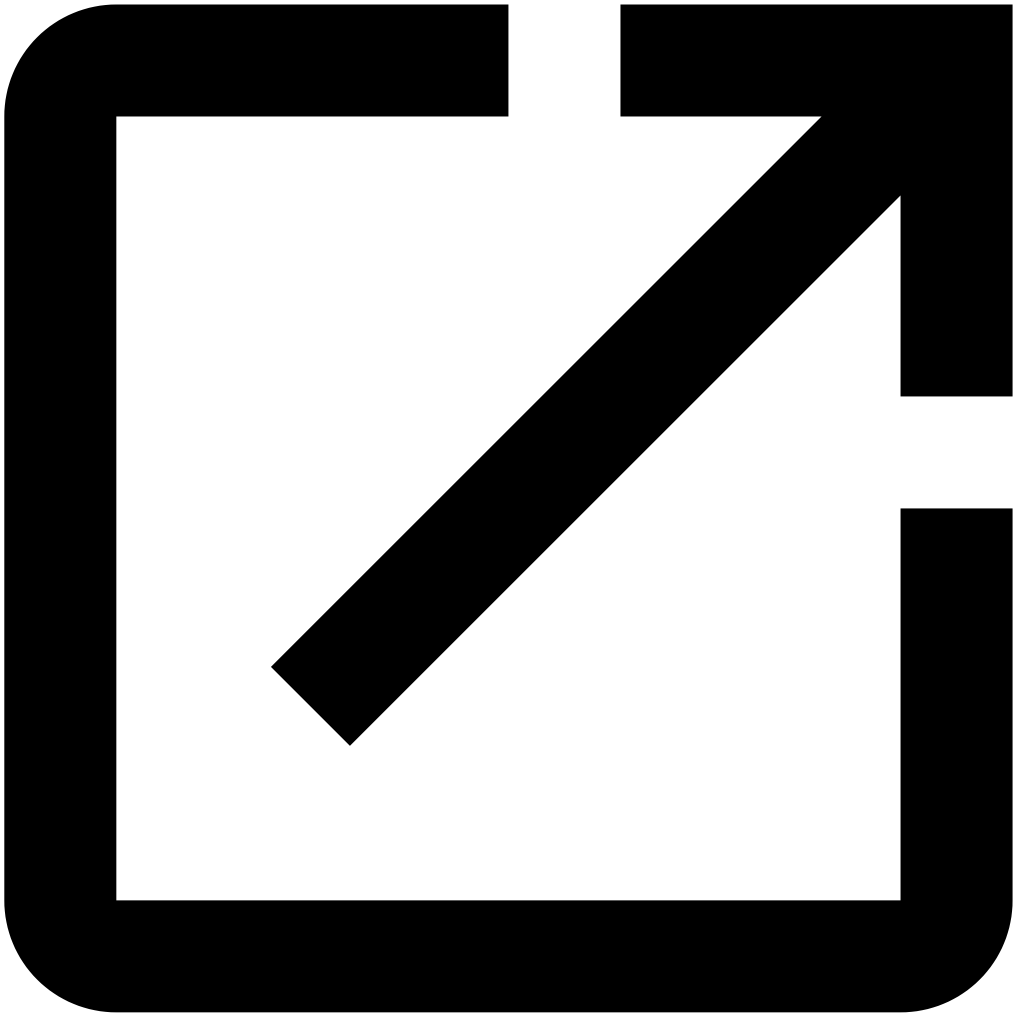
Published: 2025-07-02 · Archived: 2026-04-05 12:48:41 UTC

Australian airline Qantas disclosed that it detected a cyberattack on Monday after threat actors gained access to a third-party platform containing customer data.

Qantas is Australia's largest airline, operating domestic and international flights across six continents and employing around 24,000 people.

In a press release issued Monday night, the airline states that the attack has been contained, but a "significant" amount of data is believed to have been stolen. The breach began after a threat actor targeted a Qantas call centre and gained access to a third-party customer servicing platform.


DIE LINKE.
0:00



"On Monday, we detected unusual activity on a third party platform used by a Qantas airline contact centre. We then took immediate steps and contained the system. We can confirm all Qantas systems remain secure," Qantas stated.

"There are 6 million customers that have service records in this platform. We are continuing to investigate the proportion of the data that has been stolen, though we expect it will be significant. An initial review has confirmed the data includes some customers' names, email addresses, phone numbers, birth dates and frequent flyer numbers."

Qantas says no credit card or personal financial information was exposed, and frequent flyer account passwords, PINs, and login details were not impacted.

After detecting the breach, Qantas says it notified the Australian Cyber Security Centre, the Office of the Australian Information Commissioner, and the Australian Federal Police. It's unclear if external cybersecurity experts are assisting with the investigation.

Scattered Spider attacks target aviation firms

This attack comes as cybersecurity firms warn that hackers known as "Scattered Spider" have begun targeting the aviation and transportation industries.

While it is unclear if this group is behind the Qantas attack, BleepingComputer has learned the incident shares similarities with other recent attacks by the threat actors.

Scattered Spider (also tracked as 0ktapus, UNC3944, Scatter Swine, Starfraud, and Muddled Libra) is a group of threat actors known for their conducting social engineering and identity-based attacks against organizations worldwide, commonly using phishing, SIM swapping, MFA bombing, and help desk phone calls to gain access to employee credentials.

In September 2023, they escalated their attacks by breaching MGM Resorts and encrypting over 100 VMware ESXi hypervisors using BlackCat ransomware after gaining access by impersonating an employee. They've also partnered with other ransomware operations, such as RansomHub, Qilin, and DragonForce. Other organizations targeted by Scattered Spider include Twilio, Coinbase, DoorDash, Caesars, MailChimp, Riot Games, and Reddit.

After recently focusing on retail and insurance companies, cybersecurity firms warned on Friday that Scattered Spider had shifted its attention to aviation, with recent attacks on Hawaiian Airlines and WestJet believed to be linked to the threat actors.

BleepingComputer has learned that in the WestJet breach, threat actors exploited a self-service password reset to gain access to an employee's account, which was then used to breach the network.

The threat actors have been employing a sector-by-sector approach to their attacks, and it is unclear if they are done with the aviation sector and what industry will be targeted next.

Organizations defending against this type of threat should start by gaining complete visibility across the entire infrastructure, identity systems, and critical management services.

This includes securing self-service password reset platforms, help desks, and third-party identity vendors, which have become common targets of these threat actors.

Both Google Threat Intelligence Group (GTIG) and Palo Alto Networks have released guides on hardening defenses against the known "Scattered Spider" tactics, which admins should familiarize themselves with.

Other recent cyberattacks believed to be associated with Scattered Spider include M&S, Co-op, Erie Insurance, and Aflac.

Source: https://www.bleepingcomputer.com/news/security/qantas-discloses-cyberattack-amid-scattered-spider-aviation-breaches/