

Yakult Cyber Incident Leads to 95 GB Data Leak

DragonForce Claims the Cyber Attack

[LEARN MORE](#)



- ❖ Yakult Australia, manufacturer of a probiotic milk drink, has confirmed experiencing a "cyber incident". Both the company's Australian and New Zealand IT systems have been affected.
- ❖ Cybercrime actor DragonForce claimed responsibility for the cyber attack, and also leaked 95 GB of data that belongs to the company.
- ❖ "We first became aware of a cyber incident on the morning of the 15th of December,"
- ❖ "We cannot yet confirm the extent of the incident. We are working with cybersecurity experts to investigate the incident as a matter of urgency."
- ❖ The company was, at the time, unable to confirm how exactly the incident occurred.
- ❖ On Yakult Australia website, there was a placement of an "important message" modal that earlier in the week appeared to be blank, but now shows an incident notice.



23rd of December 2023

Yakult Australia Pty. Ltd. (Yakult Australia) advises that its Australian and New Zealand IT systems have been subject to a cyber incident.

We are working with cyber incident experts to investigate the extent of the incident.

We are currently investigating which data and systems may have been impacted.

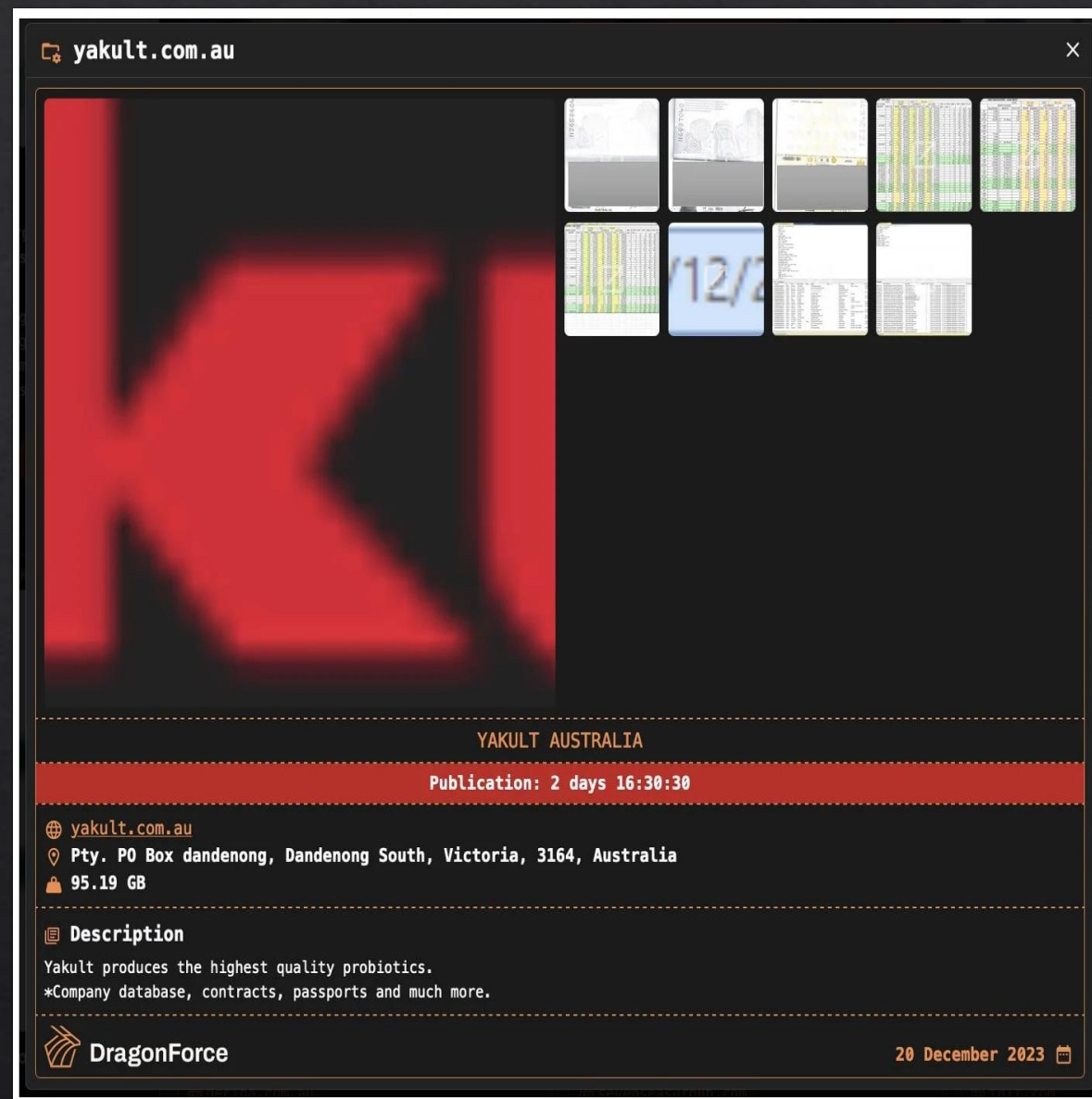
All our offices in Australia and New Zealand remain open and continue to operate.

Yakult Australia has notified the Australian Cyber Security Centre, the New Zealand National Cyber Security Centre, the Office of the Australian Information Commissioner and the Office of the Privacy Commissioner New Zealand.

Our investigations are ongoing. Further updates will be provided as information becomes available.


IMPORTANT MESSAGE FROM YAKULT AUSTRALIA


- ◇ A cybercrime actor that calls itself 'DragonForce' has taken responsibility for the incident and listed Yakult Australia to its TOR leak site on December 20th, while publicly threatening to leak 95.19 GB of data, which the group has now done.
- ◇ The data dump, according to the threat actor, contains "company database, contracts, passports and much more."
- ◇ The leaked dump appeared to contain several business documents, spreadsheets, credit applications made by Yakult Australia, employee records, and copies of identity documents such as passports.
- ◇ With its slogan, "companies that refused to cooperate," the DragonForce leak site (aka DragonLeaks) is indicative of the threat actor first attempting to extort its victims for payment failing which, it publicly leaks assets and data stolen from these companies, much like other cybercriminal groups.
- ◇ Not much information is currently known about 'DragonForce', which has listed 20 victims on its leak site thus far. The threat actor does not yet seem related to DragonForce Malaysia, a hacktivist group that has earlier targeted government agencies in the Middle East.




YAKULT AUSTRALIA

Publication: 4 days 00:52:15

 yakult.com.au

 Pty. PO Box dandenong, Dandenong South, Victoria, 3164, Australia

 95.19 GB

Description

Yakult produces the highest quality probiotics.

*Company database, contracts, passports and much more.

CYBERSECURITY (IT) INCIDENT REPORT FORM

Use this form to report any cybersecurity issues, breaches, hacks, malware, or any other incidents involving a 3rd party.

Date of Report: dec 24th, 2023

CONTACT PERSON

Full Name: Penelope Garcia Address: Canguru Ave. 32, 33rd floor

Job Title: DPO

Phone: (555) 555555 - 55555555 E-Mail: penelope.garcia@dpo.au

THE INCIDENT

Date of Incident: dec 15th, 2023 Time: 01:17 ☒ AM ☐ PM

Type of Incident: ☐ Malware ☒ Data Breach ☐ Other: _____

How was the incident detected / discovered? A cybercrime actor threatened to leak 95.19 GB of data

NOTIFICATION

Were other personnel notified? ☐ Yes ☒ No

If yes, enter: _____

CONTAINMENT

Were any containment measures made? ☐ Yes ☒ No

If yes, describe: _____

IMPACTED SERVICES

Was anything permanently impacted by the incident? ☒ Yes ☐ No

If yes, describe: Employee records, and copies of identity documents such as passports.



ATTACK VECTOR

Do you know how the attack was made? ☐ Yes ☒ No

If yes, describe: _____

INFORMATION IMPACT

Was there any data, records, or information breached? ☒ Yes ☐ No

If yes, describe: several business documents, spreadsheets, credit applications made by Yakult Australia, employee records, database, contracts, passports.

OTHER

Is there any other information you would like to include in this report? ☒ Yes ☐ No

If yes, describe: the threat actor published on a dark web forum at least some of the data he/they claim to have taken

OFFICE USE ONLY

Report received by: Aaron Hotchner Date: dec 25th, 2023

Follow-up action taken: Our investigations are ongoing. Further updates will be provided as information becomes available.

