

Exclusive: Krybit hackers claim breach of New Zealand IT services provider

By David Hollingworth

Published: 2026-04-15 · Archived: 2026-04-17 02:04:51 UTC

Ransomware new kids on the block, Krybit, has listed Auckland-based Dencom New Zealand as a hacking victim.

A newcomer to the ransomware scene has listed Kiwi company Dencom New Zealand as a victim on its darknet leak site, one of 16 victims the group has claimed to breach since it was first observed earlier this month.

Krybit listed the IT services provider on 12 April and set a ransom deadline of 22 April.

The hacker has not detailed the ransom they are seeking, but has published several documents as evidence of the hack.

The documents include personal, family correspondence of a Dencom employee, tax invoices, and medical documents – the documents date from between 2013 and 2020.

Krybit has not shared the volume of data exfiltrated during the alleged incident.

Dencom New Zealand – whose website remains inaccessible as of the time of writing – has not responded to Cyber Daily's request for comment.

Who is Krybit?

Given the group's relative junior status, not much is known about Krybit other than what it says on its leak site.

The group has positioned itself as a ransomware-as-a-service operator and is actively advertising the service online. Affiliates keep 80 per cent of any ransom proceeds, in return for the other 20 per cent, Krybit offers unlimited storage, 24/7 technical support, a fully automated malware suite, and access to a unique ransomware dashboard.

Krybit also seems to be engaged in somewhat of a turf war with another extortion operation, 0APT, which is actively attempting to extort Krybit.

"If the group does not make the payment or contact us, we will reveal their identity photos, names, location, and other," 0APT said a few days ago.

"And if you are one of their victims, contact us to get your data unlocked."

Krybit's leak site was down for maintenance as of yesterday, but is now back online and firing back at 0APT. The group has now published a list of what appears to be compromised files belonging to 0APT alongside a chatlog between the two groups.

“Next time, don’t play with the big boys,” Krybit said once its site was back up.

“The response will be fast.”

Who is Dencom New Zealand?

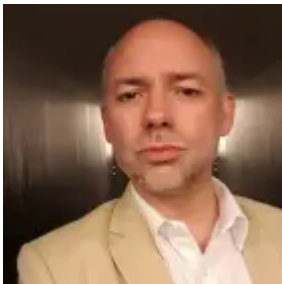
While the company’s website remains down, there are still some details to be gleaned from corporate listings on sites such as companyhub.nz. The company is a computer consulting firm and appears to operate from a residential address in Auckland, on the Te Atatu Peninsula.

Dencom New Zealand offers services including cloud backups, VOIP phone systems, web hosting, and IT hardware and software solutions.



Want to see more stories from trusted news sources?

Make Cyber Daily a preferred news source on Google.



[David Hollingworth](#)

David Hollingworth has been writing about technology for over 20 years, and has worked for a range of print and online titles in his career. He is enjoying getting to grips with cyber security, especially when it lets him talk about Lego.

Tags:

Source: <https://www.cyberdaily.au/security/13464-exclusive-krybit-hackers-claim-breach-of-new-zealand-it-services-provider>