

# Absolute Telecom Data Breach: 34GB Data Compromised

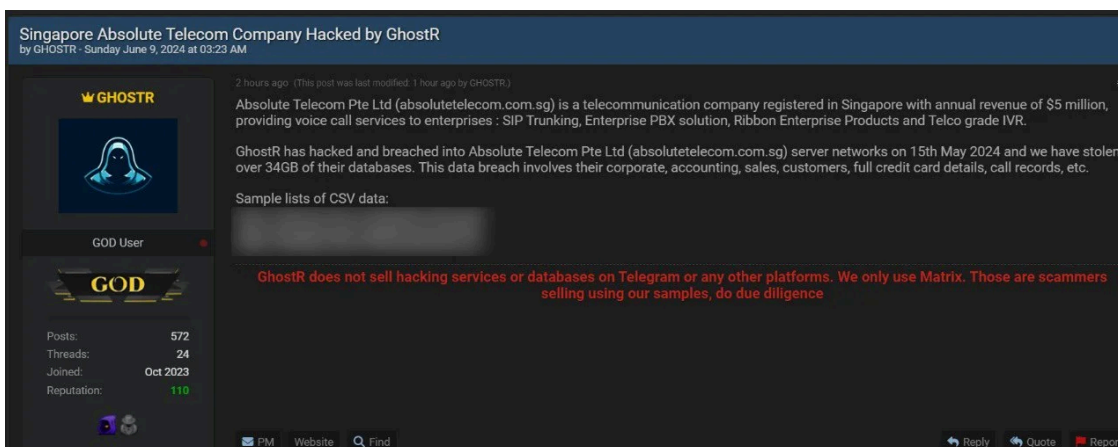
Published: 2024-06-10 · Archived: 2026-04-05 12:56:18 UTC

Absolute Telecom Pte Ltd, a prominent telecommunications company based in Singapore, has fallen victim to an alleged cyberattack.

The Absolute Telecom data breach, allegedly on May 15, 2024, has been attributed to a hacker known as “GHOSTR,” who claims to have infiltrated and compromised the company’s server networks.

This Absolute Telecom data leak has resulted in the exposure of sensitive data totaling over 34GB, including internal information such as login credentials, passwords, and subscriber details.

## Decoding the Absolute Telecom Data Breach Claims



Source: [Dark Web](#)

The compromised [data](#) in this Absolute Telecom data breach encompasses a range of crucial information, including corporate records, accounting data, sales statistics, customer particulars, full credit card details, and call records. GHOSTR, in a post on a [hacker forum](#), boasted about the successful breach and the acquisition of the extensive database belonging to Absolute Telecom Pte Ltd.

Attempts to reach out to Absolute Telecom for clarification on the extent and impact of the breach have been impeded by the unavailability of their website, which is currently offline and unresponsive.

This outage has hindered communication with the organization, leaving many questions unanswered regarding the security implications and measures being taken to address the breach.

An advertisement for CYBLE reports. It features the CYBLE logo on the left, a globe on the right, and a central text box. The main text reads "See What 2025 Really Looked Like Across Every Region". Below this, it lists regions: "Global | APAC | Europe | North America | META | Australia &amp; New Zealand". At the bottom, a red button-like area contains the text "Get Your Free Reports Today!".

After the alleged [cyberattack](#) on Absolute Telecom's website, users attempting to access the site may encounter a 'took too long to respond' error message. This service disruption indicates the impact of the breach on the company's [digital infrastructure](#), highlighting the severity of the situation and the challenges faced in restoring normalcy to their [online operations](#).

## Who is the GHOSTR Hacker Group?

GhostR, a financially driven threat actor, gained notoriety for pilfering a confidential database of 5.3 million records from World-Check. They also leaked approximately 186GB of data from a stock trading platform.

GhostR's activities on [Breachforums](#) include exposing extensive data breaches affecting Thai users, and revealing personal information like full names, phone numbers, email addresses, and ID card numbers. As of now, there are no associated families linked with this actor.

The cyberattack on Absolute Telecom underscores the persistent threat posed by malicious actors seeking to exploit [vulnerabilities](#) in digital infrastructure.

As organizations continue to rely heavily on technology to conduct their operations, safeguarding against cyber threats remains paramount to protect sensitive data and maintain the trust of customers and stakeholders alike.

This is an ongoing story and [The Cyber Express](#) will be closely monitoring the situation. We'll update this post once we have more information on the alleged Absolute Telecom data breach or any official confirmation from the organization.

*Media Disclaimer: This report is based on internal and external research obtained through various means. The information provided is for reference purposes only, and users bear full responsibility for their reliance on it. [The Cyber Express](#) assumes no liability for the accuracy or consequences of using this information.*

---

Source: <https://theycyberexpress.com/alleged-absolute-telecom-data-breach/>