

# Desorden Group Reportedly Hacks Centara Hotels & Resorts Within 10 Minutes After Recovering From the First Data Breach

---

 [seclists.org/dataloss/2021/q4/81](https://seclists.org/dataloss/2021/q4/81)

**DATA LOSS**  
**DB**

## BreachExchange mailing list archives

---

 [By Date](#) 

 [By Thread](#) 

---

*From:* Terrell Byrd <terrell.byrd () riskbasedsecurity com>

*Date:* Mon, 8 Nov 2021 13:45:45 -0500

---

<https://www.cpomagazine.com/cyber-security/desorden-group-reportedly-hacks-centara-hotels-resorts-within-10-minutes-after-recovering-from-the-first-data-breach/>

The Desorden hacking group reportedly hacked a group of luxury hotels again after a deal to pay a \$900,000 ransom collapsed.

The hacking group said it had satisfied all the hotel's demands, including providing samples of every database stolen before the management pulled out of the deal on Tuesday.

Desorden hacking group claimed to have breached the hotels again within 10 minutes and exfiltrated 400 GB of files, including personal details and the company's corporate information.

Worth \$11.6 billion, the Chirathivat family owns the Central Group that operates the Centara Hotels & Resorts that suffered the data breach.

Centara Hotels & Resorts CEO Thirayuth Chirathivat said they learned of the initial data breach that affected "a limited section of our network" on October 14.

He admitted that the hackers had accessed some customer information but not credit card and financial information. The company added that it had commenced an investigation into the data breach and would provide more information when it becomes available.

Desorden told DataBreaches.net that the hotel began its data recovery efforts and negotiation on October 16 and recovered part of the data on October 17.

However, the hacking group claims to have breached the servers again within 10 minutes to prove they still had access. It also mocked the "reputable consultant" contracted by the Centara hotels after the initial data breach.

"Reputable consultant, we will leave it for the public to think about it," the group said.

Desorden claims to have exfiltrated hundreds of gigabytes, affecting millions of customers worldwide after compromising the hotel's entire network. The group did not disclose whether the incident was a ransomware attack.

"We basically brought down their entire backend, which consists of 5 servers," Desorden claims. "In total, over 400 GB of files and data was stolen over a course of 10 days."

According to Desorden, the data breach affected millions of customers from all countries who stayed in over 70 luxury hotels operated by Central Group between 2003 and 2021. They include "luxury first-class hotel guests" and customers who made advanced bookings in 2021.

The group said that the stolen data includes name, passport number, ID number, phone, email, the residence of some hotel guests, their booking information including check-in and departure time, and other details. It also claims to have accessed "all financial data, corporate data, employee data" and other details.

Additionally, Desorden claims it hacked other companies under the Central Group management and will publish the stolen data soon.

In early October, Desorden had claimed responsibility for hacking the Central Restaurants Group in Thailand belonging to Central Group.

Earlier, the group took responsibility for hacking Acer India and leaking more than 60 GB of customer information online. Desorden subsequently hacked Acer Taiwan to make a point after warning that the company had poor cybersecurity practices and operated additional vulnerable servers in Indonesia and Malaysia.

Desorden is developing a pattern that involves mocking the victim and apparently executing follow-up attacks to make a point. However, the success of the initial and follow-up attacks seems to bolster Desorden's credibility.

---

BreachExchange mailing list sponsored by Risk Based Security  
BreachExchange () lists riskbasedsecurity com

If you wish to Edit your membership or Unsubscribe you can do so at the following link:  
<https://lists.riskbasedsecurity.com/listinfo/breachexchange>

---

← [By Date](#) →

← [By Thread](#) →

**Current thread:**

---

**Desorden Group Reportedly Hacks Centara Hotels & Resorts Within 10 Minutes After Recovering From the First Data Breach** *Terrell Byrd (Nov 10)*