Nordic Choice Hotels hit by Conti ransomware, no ransom demand yet

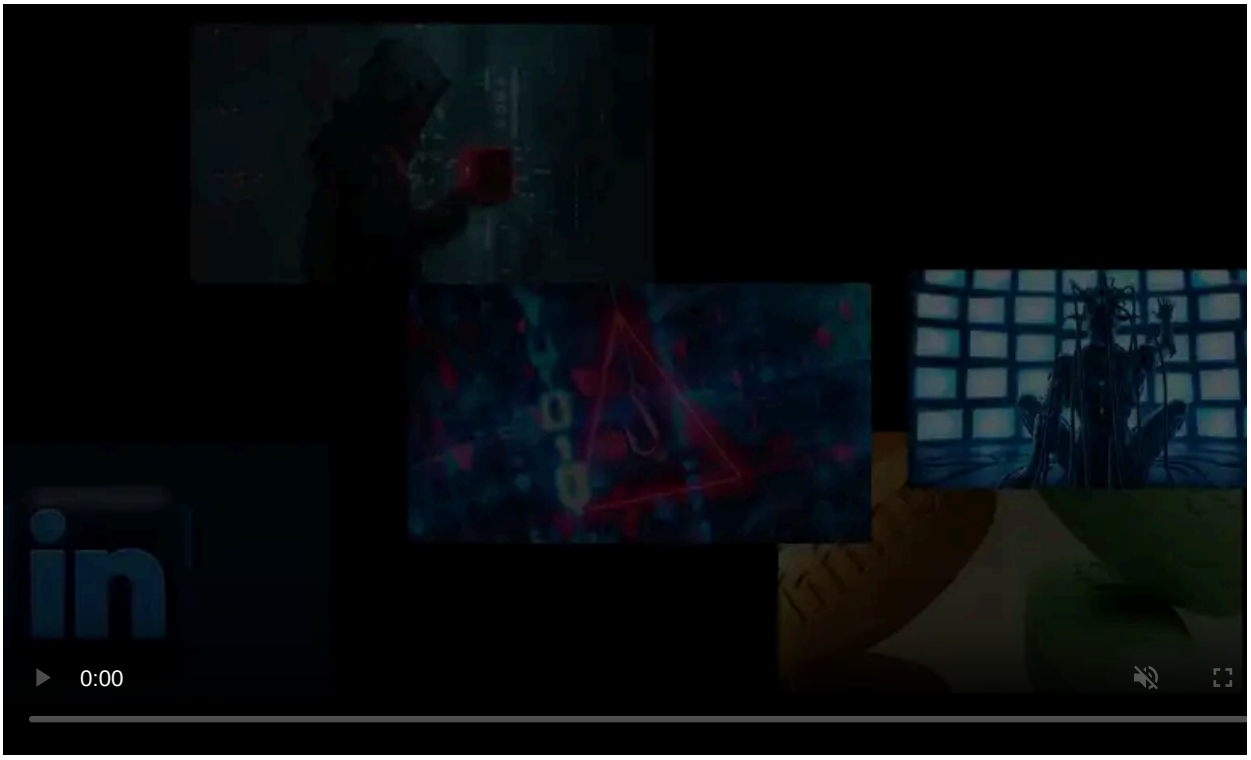
By Ax Sharma

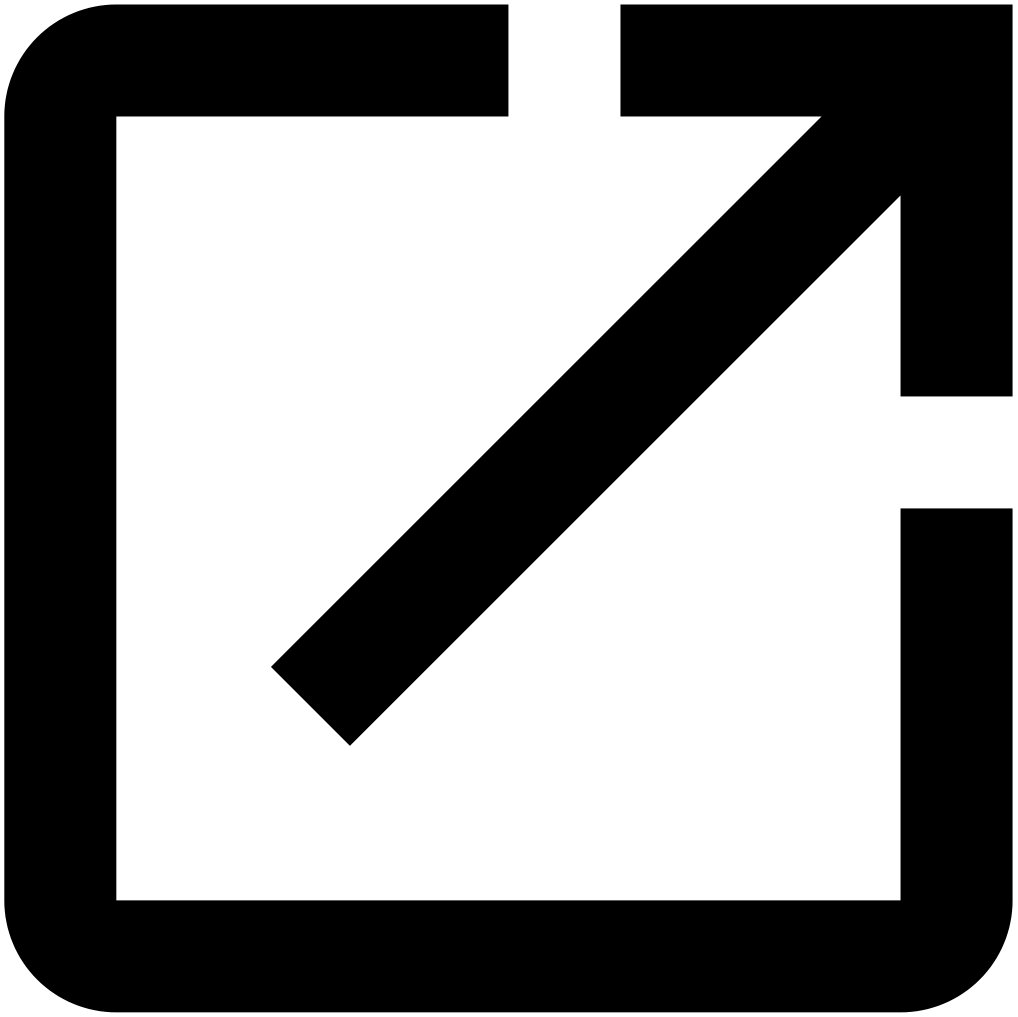
Published: 2021-12-07 · Archived: 2026-04-05 17:52:23 UTC

Nordic Choice Hotels has now confirmed a cyber attack on its systems from the Conti ransomware group.

The incident primarily impacts the hotel's guest reservation and room key card systems.

Although there is no indication of passwords or payment information being affected, information pertaining to guest bookings was potentially leaked.


0:00



The Scandinavian hotel chain, with its brands—Comfort, Quality, and Clarion, employs over 16,000 staff members and has 200 properties across Scandinavia, Finland, and the Baltics.

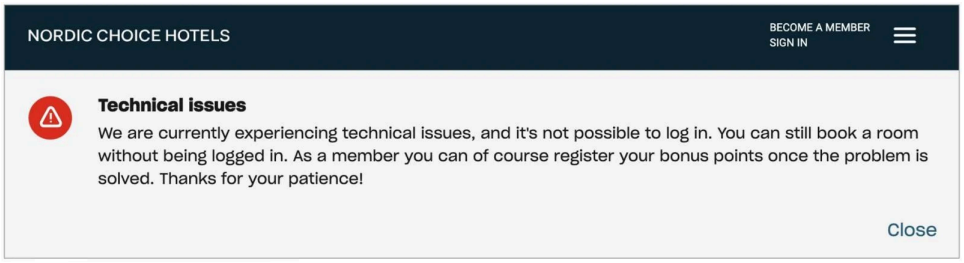
Key cards out of service

Earlier this week, Nordic Choice Hotels group announced its IT systems were hit by a "computer virus" on Thursday, December 2nd.

The incident left the hotel staff without access to the hotel's reservation systems that manage check-in, check-out, payments, and bookings.

Although the staff switched to manual procedures to carry out business operations, the hotel advised guests that delays are to be expected.

Members are currently unable to log in to their Nordic Choice Hotels accounts to book and manage reservations, or apply reward points, although it remains possible to book stays without being logged in:



Nordic Choice Hotels systems still facing 'technical issues' (BleepingComputer)

A subsequent blog post by the hospitality group confirmed the scope of the incident expands to Nordic Choice Club members, in addition to the current hotel guests.

One of the hotel guests, security researcher Runa Sandvik also reported key cards being out of service:

No ransom demand yet, law enforcement engaged

Law enforcement agencies including the Norwegian Data Protection Authority and the Norwegian National Security Authority were notified of the attack by the hotel company on December 2nd—the same day as the attack.

"Our investigations do not currently give any indication that data has been leaked, but we can't guarantee that is the case. Therefore, the incident entails a risk that information about the guests' bookings may be lost," explains the company in a release.

"This information consists of name, email address, telephone number, date of the visit and any information the guest may have provided in connection with their visit. There is no indication that card or payment information has been leaked."

Although the hospitality group cannot be sure of any data leak just yet, the decision to be transparent and inform its members of the incident is an effort to keep them alerted against any suspicious communications—texts, messages, phone calls, or emails, that may be directed at them.

At this time, the hotel group has "chosen not to contact" the threat actors behind the attack, nor have they received a ransom demand from the Conti ransomware group.

BleepingComputer also did not come across the hotel group's name on Conti's data leak pages, indicating the ransomware attack is in early stages and negotiations may not have begun yet.

Conti ransomware is a private Ransomware-as-a-Service (RaaS) operation believed to be controlled by a Russian-based cybercrime group known as Wizard Spider.

Conti shares some of its code with the notorious Ryuk Ransomware, whose TrickBot distribution channels they started using after Ryuk activity decreased around July 2020.

This ransomware gang has previously targeted over a dozen healthcare and first responder organizations, and police department systems.

Earlier this year, Conti breached networks of Ireland's Health Service Executive (HSE) and Department of Health (DoH), asking the former to pay a $20 million ransom after successfully encrypting its systems.

"Over the weekend, we have managed to put in place replacement solutions at most of our hotels. The work is now in full swing to get everyone back into normal operation, something we think will be done within the next few days," says Bjørn Arild Wisth, Deputy CEO at Nordic Choice Hotels.

During the next few days, as the company works with law enforcement to remediate the cyber attack, some hotel properties may continue to experience delays with regards to check-in, check-out, and reservation processes.

"Our customer center currently has limited opportunity to change and add bookings, but is in place to be able to answer any questions. In that case, we recommend that you send us an email at booking@choice.no or use our website for further information," advises Nordic Choice Hotels.

Source: https://www.bleepingcomputer.com/news/security/nordic-choice-hotels-hit-by-conti-ransomware-no-ransom-demand-yet/