Wind turbine firm Nordex hit by Conti ransomware attack

By Lawrence Abrams

Published: 2022-04-15 · Archived: 2026-04-06 00:55:51 UTC

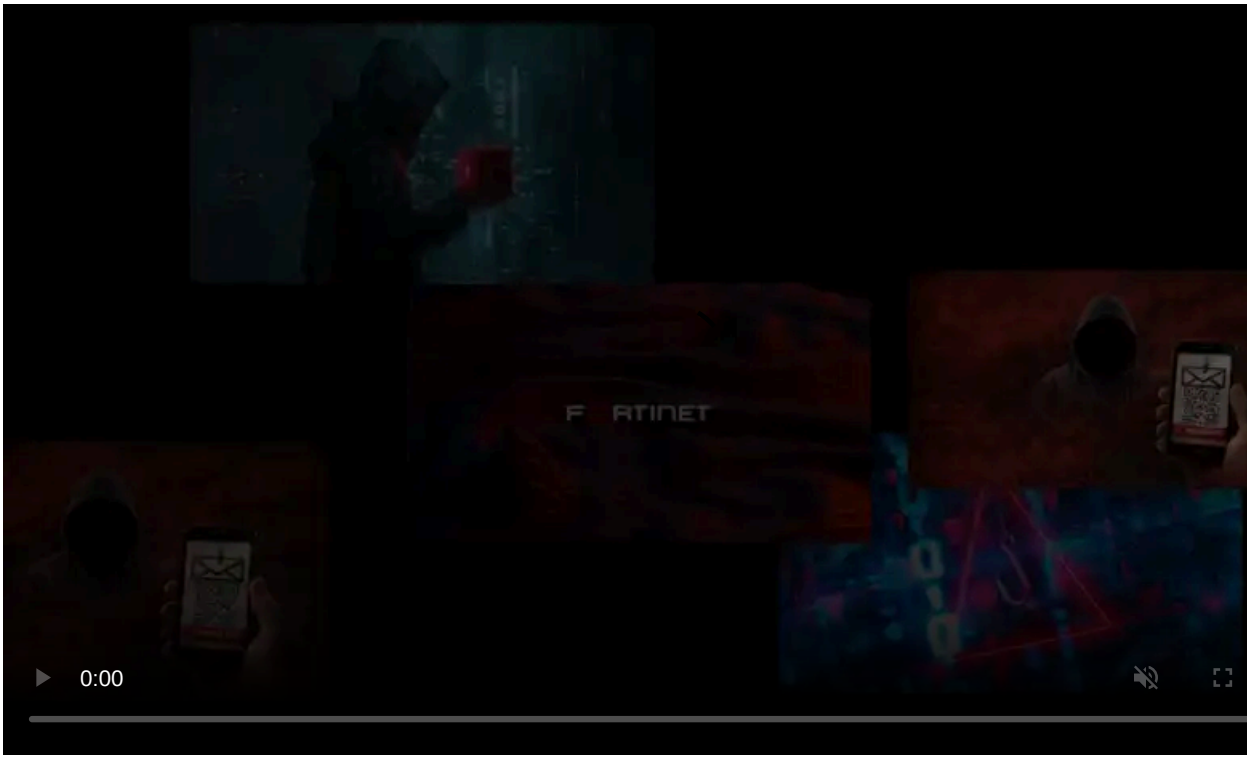
Image: Nordex

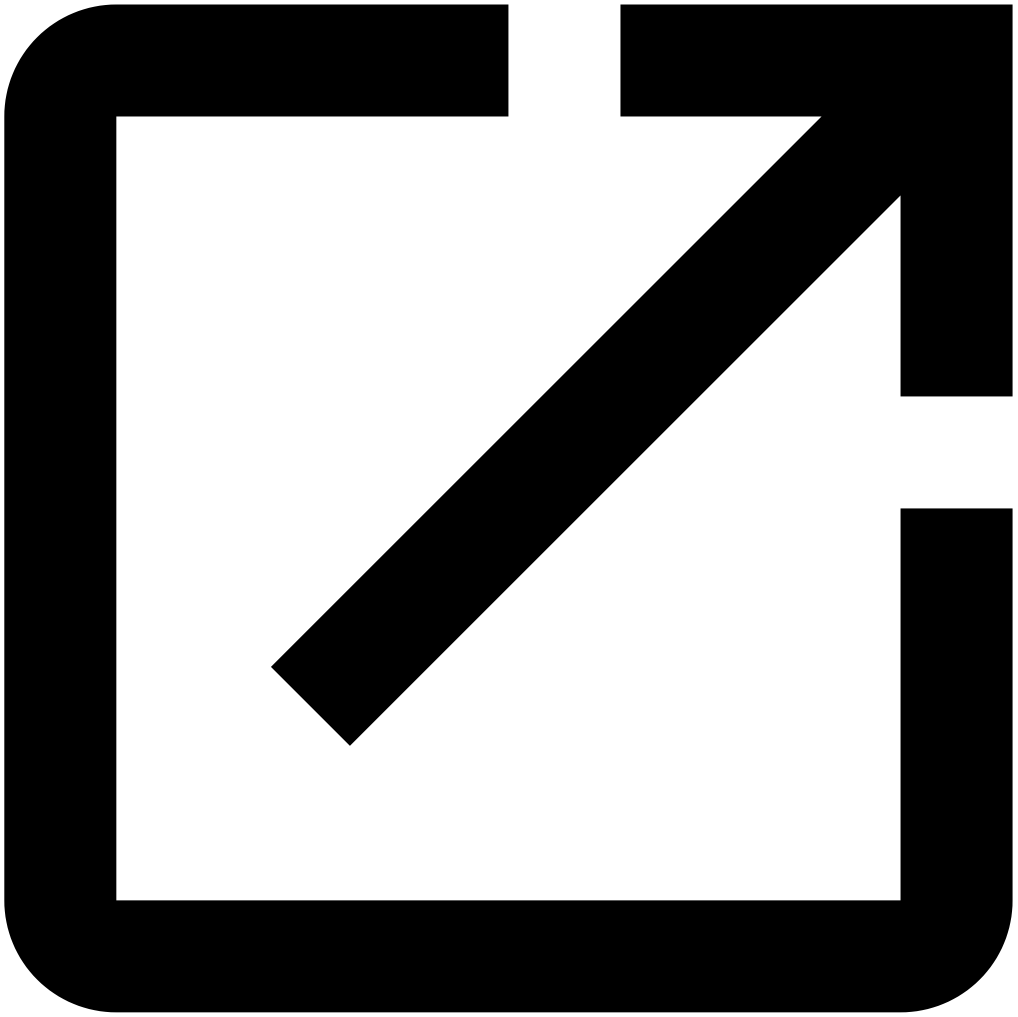
The Conti ransomware operation has claimed responsibility for a cyberattack on wind turbine giant Nordex, which was forced to shut down IT systems and remote access to the managed turbines earlier this month.

Nordex is one of the largest developers and manufacturers of wind turbines globally, with more than 8,500 employees worldwide.

On April 2nd, Nordex disclosed that they had suffered a cyberattack that was detected early and that the company had shut down its IT systems to prevent the spread of the attack.

"The intrusion was noted in an early stage and response measures initiated immediately in line with crisis management protocols. As a precautionary measure, the company decided to shut down IT systems across multiple locations and business units," explained Nordex's original press statement.


F RTINET
0:00



However, BleepingComputer was told on March 31st that the company suffered a Conti ransomware attack which caused the entire platform to go offline. Our source further said that Nordex did not know where the attack was coming from and was starting their investigations.

Multiple emails sent by BleepingComputer to Nordex to confirm if they suffered a ransomware attack have remained unanswered.

Yesterday, Nordex released an updated statement explaining that they had also disabled remote access to managed turbines to safeguard customers' assets.

They further state that their investigation shows that the attack was restricted to their own internal systems and did not spread to customers' assets.

"In close cooperation with relevant authorities, the emergency response team of internal and external IT experts has been performing extensive investigations and forensic analysis," reads Nordex's update on the cyberattack.

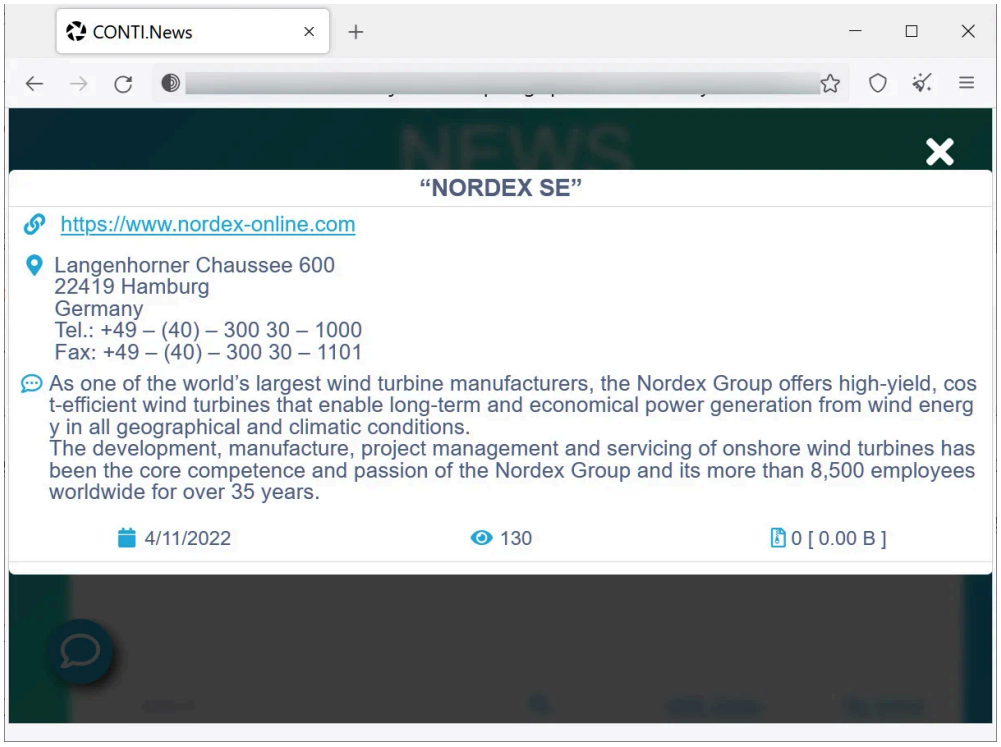
"Preliminary results of the analysis suggest that the impact of the incident has been limited to internal IT infrastructure. There is no indication that the incident spread to any third-party assets or otherwise beyond Nordex' internal IT infrastructure"

Danish wind turbine producer Vestas suffered a ransomware attack last November by the LockBit ransomware operation.

Conti ransomware claims attack on Nordex

Today, the Conti ransomware operation claimed that they were behind the attack on Nordex.

However, the ransomware gang has not begun leaking any data, indicating that the company may be negotiating with the threat actors or that no data was stolen during the attack.



Conti ransomware claims attack on Nordex

Conti is an elite ransomware operation operated by a Russian hacking group known for other notorious malware infections, including Ryuk, TrickBot, and BazarLoader.

Conti commonly gains access to a corporate network after a device becomes infected with the BazarLoader or TrickBot malware infections through a phishing attack.

While spreading through a network, the threat actors will steal files and upload them back to their servers.

This data is then used as part of double-extortion attacks to pressure victims into paying a ransom.

The Conti gang recently suffered its own data breach after a Ukrainian researcher published almost 170,000 internal chat conversations between the Conti ransomware gang members and the Conti ransomware source code.

Due to the cybercrime gang's ongoing activity, the US government issued an advisory on Conti ransomware attacks.

Source: https://www.bleepingcomputer.com/news/security/wind-turbine-firm-nordex-hit-by-conti-ransomware-attack/