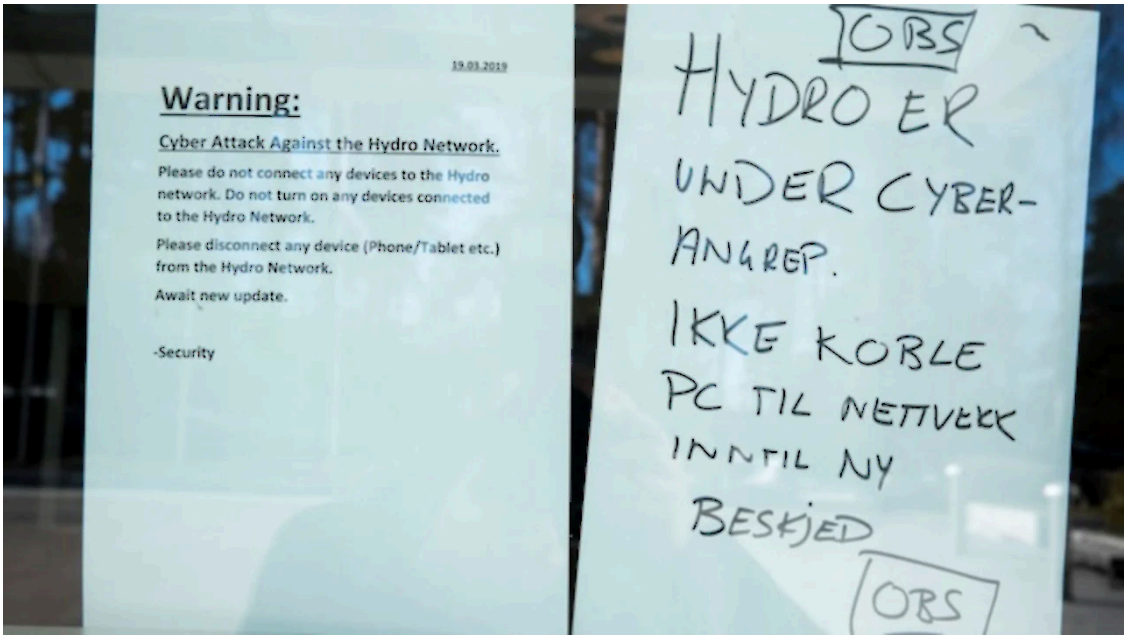
LockerGoga Ransomware Sends Norsk Hydro Into Manual Mode

By Ionut Ilascu

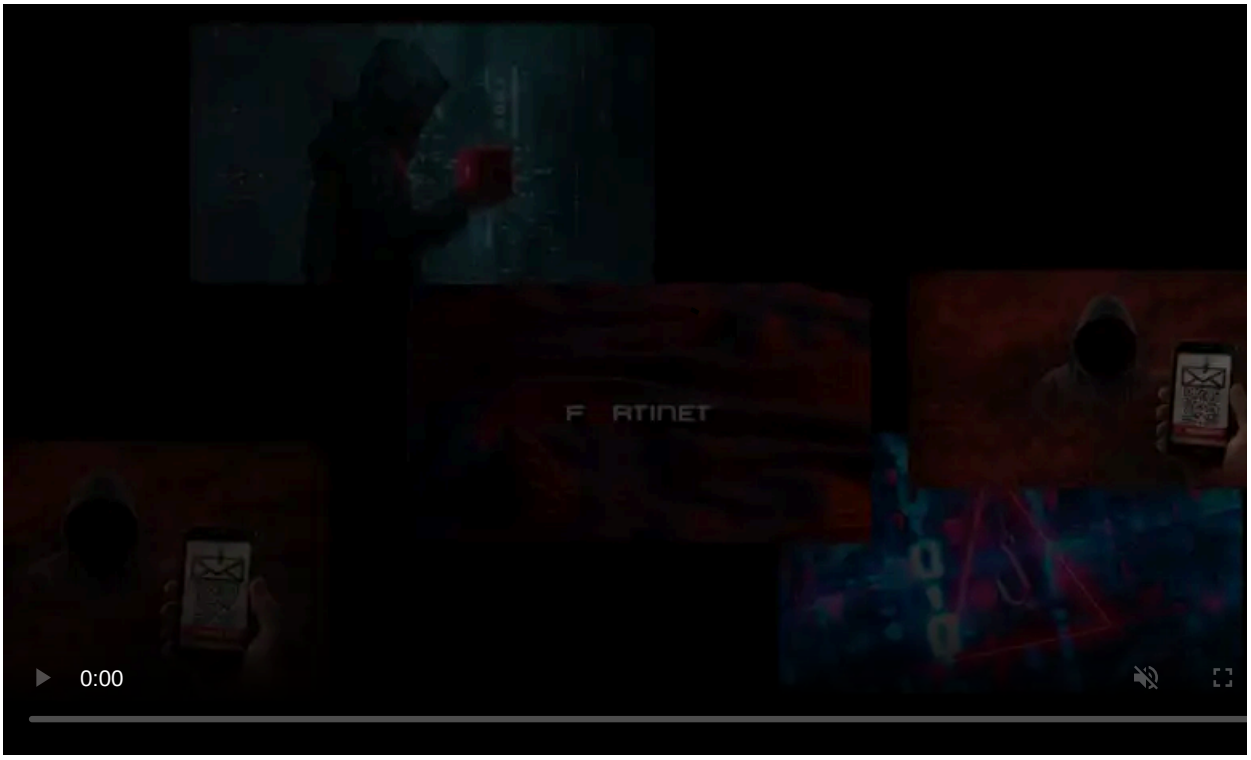
Published: 2019-03-19 · Archived: 2026-04-05 22:25:38 UTC

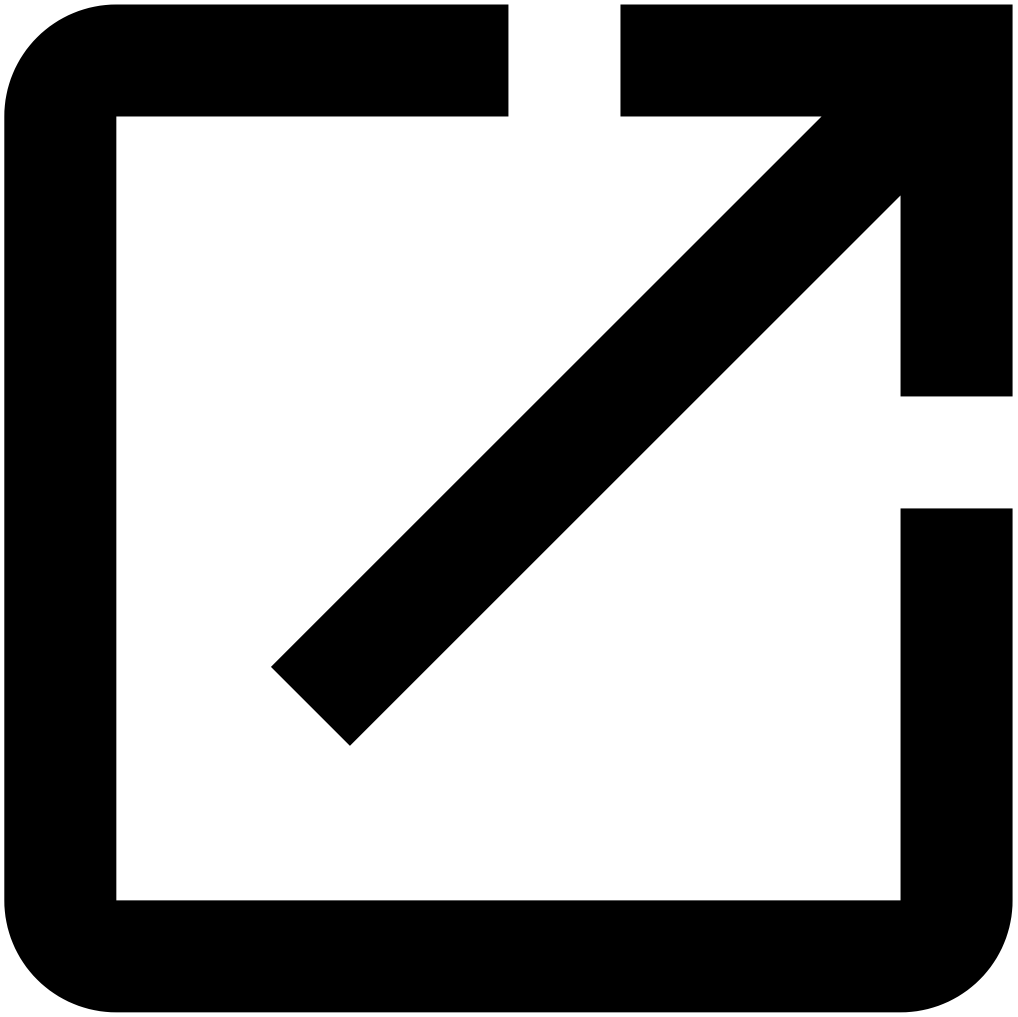


One of the largest aluminum producers in the world, Norsk Hydro, has been forced to switch to partial manual operations due to a cyber attack that is allegedly pushing LockerGoga ransomware.

The company announced today that it is the target of an extensive cyber attack that was noticed by the IT staff noticed late Monday (around midnight), CET, affecting computer systems in most business areas.

LockerGoga ransomware is relatively new on the scene. Although it has made multiple victims, it gained public attention in January in an attack against Altran Technologies, an engineering consulting firm operating at a global level, headquartered in Paris, France.


F RTINET
0:00



NorCERT warns companies on LockerGoga attack

According to media outlet NRK, NorCERT alerted a number of partners about LockerGoga ransomware, warning that Norsk Hydro is one of its victims.

The notification from Norway's cybersecurity body says that the attack involved Active Directory - used for authenticating and authorizing all users and systems on a Windows domain type network.

"NorCERT warns that Hydro is exposed to a LockerGoga attack. The attack was combined with an attack on Active Directory (AD)," reads the alert.

However, Håkon Bergsjø, head of NorCERT, would not confirm for NRK that the attack targeted Active Directory servers in the case of Norsk Hydro.

BleepingComputer reached out to NorCERT but received no reply at the time of publishing.

In an 18-minute press conference today, the director of the Norwegian cybersecurity authority declined to publicly name LockerGoga as the culprit for the attack on Hydro. However, the director said that an infection with this ransomware is one of the theories.

Information about the malware is now collected through collaboration at national and international level.

Norsk Hydro mum on attack details

In public statements today, Norsk Hydro did not comment on the nature of the attack but described a critical situation of an ongoing event, saying that they "are working to contain and neutralize the attack" with external help.

The company has notified the relevant authorities and informed in an official update on Facebook that it "is switching to manual operations where possible."

Eivind Kallevik, Norsk Hydro CFO Eivind Kallevik during the press conference confirmed the ransomware infection. Describing the situation as "quite severe," the CFO added that good backup solutions and routines are in place. The main strategy is to rely on them to restore all operations to normal and avoid paying the ransom.

Production losses are minimal, the Kallevik stated. Some facilities are running in manual mode, which implies more people working in multiple shifts.

People have not been endangered as a result of the cyber attack, which impacted operations in several business areas around the globe.

As of today, the company is able to process all customer order and deliver on them. However, future requests might be affected because the entire network is currently down - the company website shows a 404 error.. Until the problem is solved, the company has been organized to work 24/7.

The main priority at the moment is to ensure safe operations, limit operational and financial impact, to clean the infected servers and to reinstall them from backups.

There is no indication that power plants outside Norway are affected by the incident as all of them have been isolated from the company's global network.

Update [03.19.19, 11AM EST]: Norsk Hydro held a press conference to offer details about the cyberattack on its network. The article has been updated with new information from the company's CFO Eivind Kallevik and the director of the Norwegian cybersecurity authority.
