String of cyberattacks on European oil and chemical sectors likely not coordinated, officials say

By Adam Janofsky

Published: 2023-01-17 · Archived: 2026-04-05 20:03:12 UTC

European prosecutors and cybersecurity officials are investigating a ransomware attack affecting several major oil port terminals that occurred just days after a separate hack on two German companies forced oil suppliers to reroute their products to alternative depots.

The attacks targeted organizations in Belgium, the Netherlands, and Germany, including some of the largest ports in the region. Cybersecurity officials from those countries on Thursday said they do not have reason to believe that the attacks are linked to one another.

One European government official who is involved in the investigation but is not authorized to speak about it publicly told The Record that the port incidents are ransomware attacks believed to be linked to the BlackCat and Conti families. An internal report from Germany's Federal Office for Information Security (BSI) said the BlackCat group, which has been implicated in a number of recent compromises, was behind the recent attack on the two German oil industry companies, Handelsblatt reported on Wednesday.

"A judicial investigation is ongoing at the public prosecutor's office in Antwerp. Attribution of such a cyberattack is, as you know, very difficult and it is now far too early for that. We have no technical indications that the attacks are linked," Katrien Eggers, a spokesperson for the Centre for Cyber Security Belgium, told The Record. The Centre serves as the country's central authority for cybersecurity.

The Netherlands' National Cyber Security Center said in a statement that it does not believe the attacks targeting the oil and chemical sector in the Netherlands, Belgium and Germany to be related, and that it does not appear to be linked to nation-state hackers.

"The NCSC's view is that at the moment there does not seem to be a coordinated attack and that the attacks were probably committed with a criminal motive. The NCSC is closely monitoring developments and will take further action if necessary."

According to De Tijd, a Belgian newspaper that first reported on the port cyberattacks, Ghent-based Sea-Invest suffered an attack that caused activities at its terminals worldwide to come to a standstill. The company has 5,500 employees and handled more than 150 million tons of goods last year, according to the paper.

In a statement in Dutch emailed to The Record, the company confirmed that attackers crippled Sea-Invest's networks the night of Jan. 30 with ransomware. It added that its dry bulk division did not have to cease operations and that its liquid bulk department, Sea-Tank, has been able to resume operations as of yesterday evening.

Rerouting oil supplies

Earlier in the week, a cyberattack on Oiltanking GmbH and Mabanaft GmbH — two subsidiaries of the German logistics firm Marquard & Bahls — caused Shell to reroute oil supplies to other depots.

"On Saturday, January 29th 2022, [Oiltanking and Mabanaft] discovered we have been the victim of a cyber incident affecting our IT systems," a company spokesperson told The Record in a statement. "Upon learning of the incident, we immediately took steps to enhance the security of our systems and processes and launched an investigation into the matter. We are working to solve this issue according to our contingency plans, as well as to understand the full scope of the incident. We are undertaking a thorough investigation, together with external specialists and are collaborating closely with the relevant authorities. All terminals continue to operate safely."

The spokesperson added that a unit of Manabaft that operates all terminals in Germany is operating with limited capacity and has declared force majeure, meaning it cannot fulfill its prior agreements due to unforeseeable circumstances.

Attacks on oil and gas infrastructure have always been a top concern for the public and private sector, but came into focus last May when a ransomware attack on Colonial Pipeline disrupted the supply of gasoline and jet fuel to major parts of the Southeast.

The Biden Administration blamed the attack on the DarkSide ransomware group, which soon shut down operations. Last month, a senior Biden administration official said an REvil hacker arrested by Russia's security service was responsible for the attack.

No previous article

No new articles

Adam Janofsky

is the founding editor-in-chief of The Record from Recorded Future News. He previously was the cybersecurity and privacy reporter for Protocol, and prior to that covered cybersecurity, AI, and other emerging technology for The Wall Street Journal.
