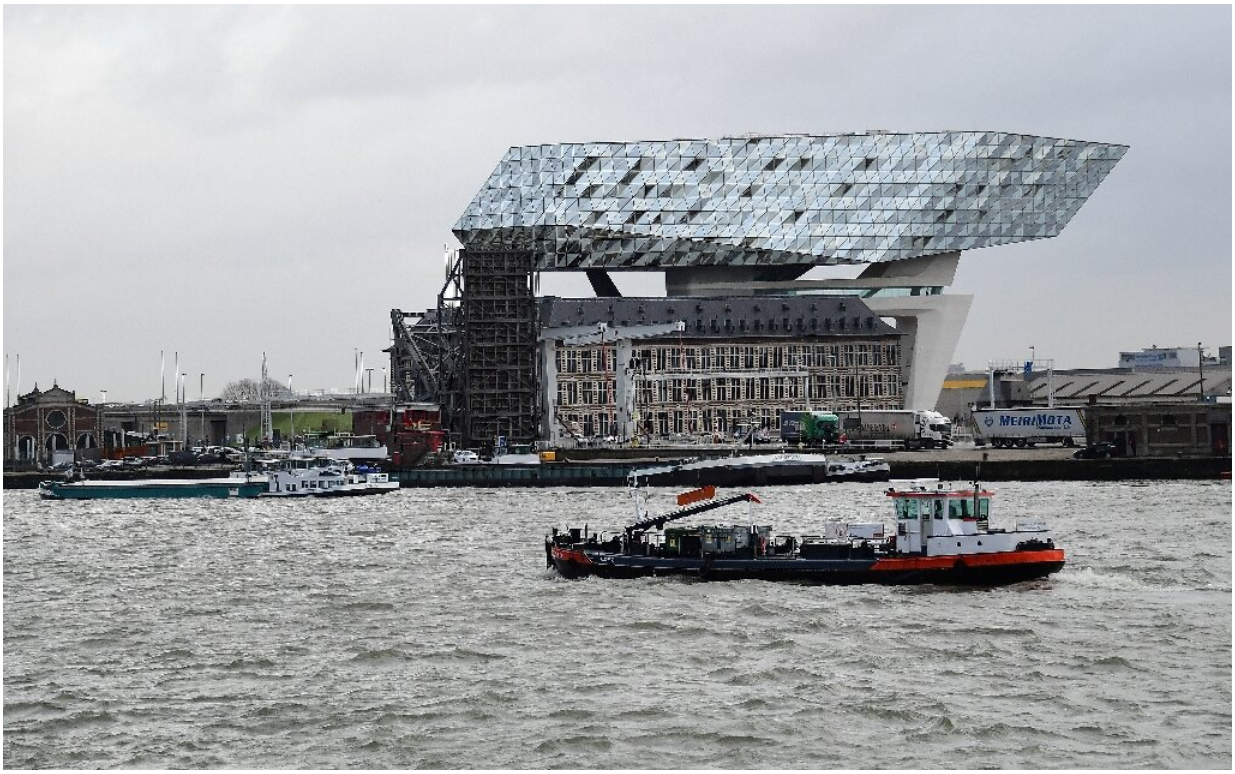
European oil port terminals hit by cyberattack

February 3 2022, by Matthieu Demeestere With Afp Bureaux



Belgium's main port, Antwerp, was one of those where oil trading firms systems were hacked by suspected ransomware attackers.

Major oil terminals in some of Western Europe's biggest ports have fallen victim to a cyberattack at a time when energy prices are already soaring, sources confirmed on Thursday.

Belgian prosecutors have launched an investigation into the hacking of oil facilities in the country's maritime entryways, including Antwerp, Europe's second biggest port after Rotterdam.

In Germany, prosecutors said they were investigating a cyberattack targeting oil facilities in what was described as a possible ransomware strike, in which hackers demand money to reopen hijacked networks.

Oil prices hit a seven-year high last month amid diplomatic tensions with gas supplier Russia, and energy bills are fuelling a rise in inflation that has spooked European policymakers.

According to a specialised broker, the alleged hacking is affecting several European ports and is disrupting the unloading of barges in this already strained market.

"There was a cyberattack at various terminals, quite some terminals are disrupted," said Jelle Vreeman, senior broker at Riverlake in Rotterdam.

"Their software is being hijacked and they can't process barges. Basically, the operational system is down," he said.

The EU's Europol police agency said it was aware of the incidents in Germany and had offered support to authorities.

"At this stage the investigation is ongoing and in a sensitive stage," Europol spokeswoman Claire Georges said.

One of the main victims seems to be the cross-border Dutch and Belgian Amsterdam-Rotterdam-Antwerp oil trading hub, where company IT systems were affected by the attack.

SEA-Tank Terminal, which has storage facilities in Antwerp, was hit,

Belgian daily De Morgen reported.

The Dutch National Cyber Security Centre said the attacks were "probably committed with a criminal motive" and pledged to take further action "if necessary".

'Not grave'

In Germany, two oil supply companies said they were victim to the cyberattack since Saturday January 29.

Both Oiltanking Deutschland GmbH and Mabanaft declared force majeure, an emergency legal clause that is used when a company cannot fulfil its supply contracts because of an unforeseeable event, a joint statement said.

"We are committed to resolving the issue and minimising the impact as quickly and effectively as possible," they said.

The head of Germany's IT security agency, Arne Schoenbohm, said at a conference on Tuesday that the incident was serious but "not grave", German media reports said.

According to the German newspaper Handelsblatt, an initial report from German security services identifies the BlackCat ransomware as the tool used in the cyberattack in Germany.

BlackCat emerged in mid-November 2021 as a software tool to allow hackers to seize control of target systems and has quickly gained notoriety for its sophistication and innovation.

According to US cybersecurity firm PaloAlto, BlackCat has the added advantage of being more lucrative than its rivals for the hackers who use

it—other ransomware platforms usually take a higher commission.

The experts also note that BlackCat's programmers use the Russian language, but this clue could be misleading since hackers often leave false clues to cover their tracks.

Recent ransomware attacks against targets in the United States and other western countries have been blamed on Russian-speaking hacker groups or those operating from Russian territory.

In June, US authorities said they had recovered a ransom payment paid by Colonial Pipeline to Russia-based ransomware extortionists Darkside, who had forced the shutdown of a major fuel network.

The attack caused short-term fuel shortages and drew attention to the broader threat that ransomware posed to essential infrastructure and services.