Maersk sheds two more offshore support vessels

Danish drilling contractor Maersk Drilling has sold two anchor handlers, the Maersk Puncher and Maersk Purpose, as it continues trimming its OSV fleet. In May, Maersk Supply Service announced it had sold two more offshore vessels as part of its ongoing divestment strategy.

Russian and Indonesian oil companies

Rosneft and Pertamina have signed an agreement for cooperation in offshore oil and gas exploration. The companies have been discussing cooperation in the hydrocarbon sector for several years and the agreement is part of that ongoing dialogue.

Rosneft's Chayvo field

Russia's Rosneft has found an oil field in the Khatanga Bay of the Laptev Sea, in what is considered to be an important discovery. The field, known as Chayvo, is expected to result in a large oil production volume over the long term.

Rosneft buys into Eni's giant gas discovery

Danish drilling contractor Maersk Drilling has been hit as part of a global cyber-attack named Petya on the 27 June. The company, which provides services to the oil and gas industry, has revealed that their IT systems are down across multiple sites and select business units. They have confirmed that Maersk has been hit as part of the attack.

Events

In an update on Tuesday, Kaspersky Labs said: "The company's telemetry data indicates around 2,000 attacked users so far. Organizations in Russia and the Ukraine are the most affected, and we have confirmed that a modified ransomware as publically reported, but a new ransomware that has not been seen before. That is something new, never seen before."

"Kaspersky Lab's analysts are investigating the new wave of ransomware attacks targeting companies around the world. The exploit is being actively used to infect the operating systems of systems not yet patched.

"The attack appears to be a complex attack which involves several attack vectors. We can confirm that a modified ransomware is being used. Initially, the attackers used a backdoor to access the system, and then used it to spread the ransomware."

"Instead of encrypting files one by one, it denies access to the full system by attacking low-level structures on the disk. This ransomware's authors have not only created their own boot loader but also used the boot loader exploit to start the attack.

"We have contained the attackers and recovered some data. However, we are still investigating to understand the extent of the attack.

"The cyber attack could lead to serious consequences, however, due to the scale of the attack. We are working with our partners to contain the attack and are investigating how it can be prevented in the future."

In an interview with Reuters, Rosneft said: "We are working with our partners to contain the attack and are investigating how it can be prevented in the future."

Rosneft production not affected

Rosneft production not affected by cyber-attack. The Russian oil giant reported that several other organizations have been hit, including the Russian oil giant Rosneft, and said: "Rosneft production not affected."

"We have been working with our partners to contain the attack and are investigating how it can be prevented in the future."

"Rosneft production not affected."

"We are working with our partners to contain the attack and are investigating how it can be prevented in the future."

On Wednesday afternoon, Rosneft tweeted: "The large scale cyber attack has not affected Rosneft production. Preparation processes were stopped."

Additionally, Rosneft said: "The cyber attack could lead to serious consequences, however, due to the scale of the attack. We are working with our partners to contain the attack and are investigating how it can be prevented in the future."

"Rosneft production not affected.

"We are working with our partners to contain the attack and are investigating how it can be prevented in the future."

"Rosneft production not affected."

"We are working with our partners to contain the attack and are investigating how it can be prevented in the future."