

## Marine services provider Swire Pacific Offshore hit by ransomware

By Bill Toulas

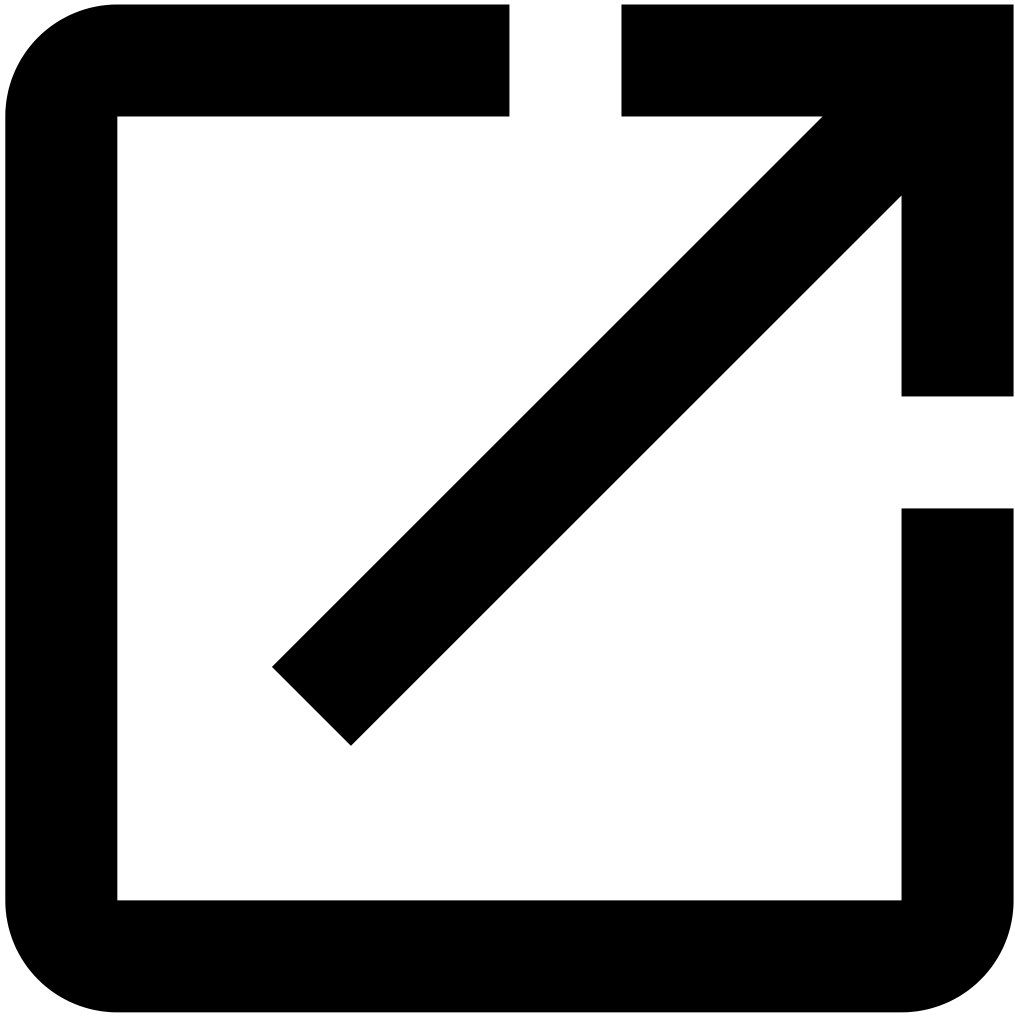
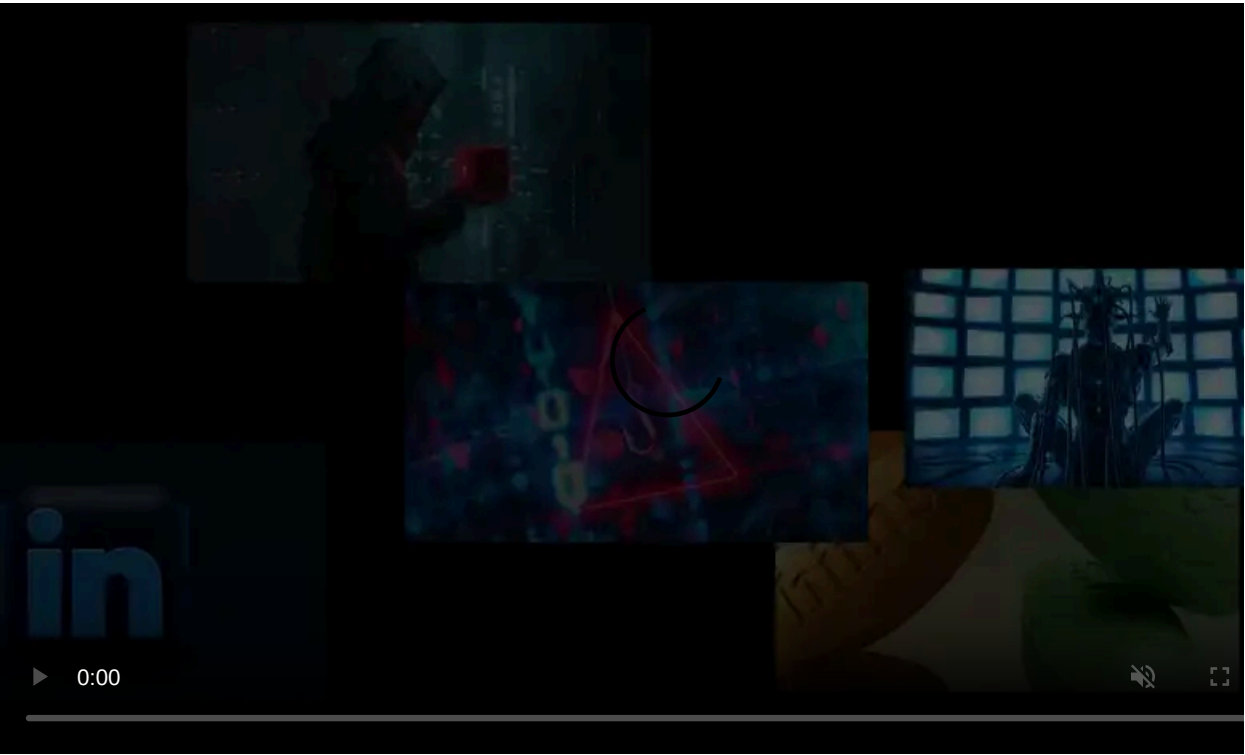
Published: 2021-11-26 · Archived: 2026-04-05 17:36:42 UTC



Marine services giant Swire Pacific Offshore (SPO) has suffered a Clop ransomware attack that allowed threat actors to steal company data.

Swire Pacific Offshore discovered an unauthorized network infiltration onto its IT systems, resulting in the compromise of some employee data.

"Swire Pacific Offshore (SPO) has discovered that it was the target of a cyberattack which involved unauthorised access to its IT systems," Swire Pacific Offshore said in a [statement](#) to BleepingComputer.



Visit Advertiser website [GO TO PAGE](#)

"The unauthorised access has resulted in the loss of some confidential proprietary commercial information and has resulted in the loss of some personal data. The cyberattack has not materially affected SPO's global operations."

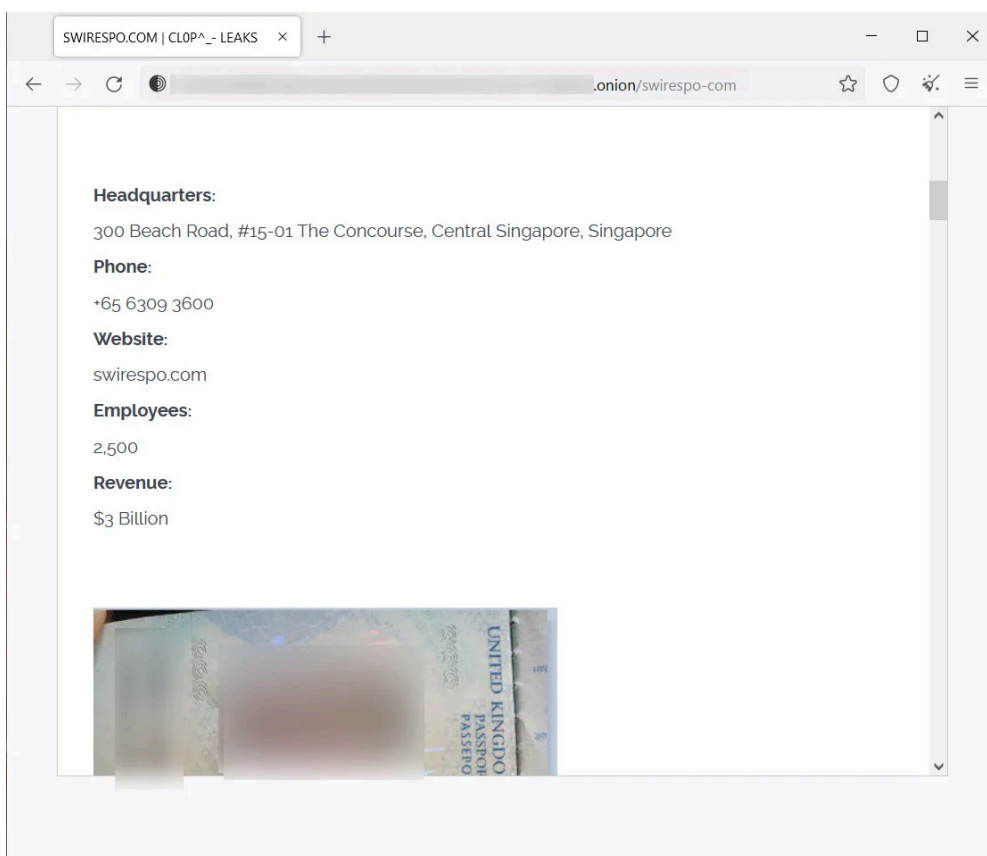
As the company clarified, the cyberattack hasn't affected SPO's global operations, and neither has it resulted in the loss of confidential information.

The firm has reported the incident to the relevant authorities and continues to investigate with the help of external experts to determine the exact scope and impact.

## Clop gang claims responsibility

The Clop ransomware group has claimed responsibility for the attack and posted screenshots of data during the attack.

The screenshots indicate that the ransomware gang stole passports, payroll information, ID numbers, bank account details, email addresses, and internal correspondence messages.



**Swire Pacific page on Clop data leak site**

From what BleepingComputer could discern by the leaked data, the claims that the threat actors stole employees' personal data during the attack appear valid.

## Size of the breach

The number of exposed individuals could reach 2,500, corresponding to the firm's seafaring and onshore personnel in 18 countries.

SPO will contact all of the potentially affected individuals to inform them about the incident, but no exact numbers have been published yet.

Swire Pacific Offshore is a Singapore-based maritime services provider which operates a fleet of over 50 offshore support vessels.

## Targeting the shipping industry

Ransomware actors always aim for costly business disruptions, as this raises the chances of them receiving the ransom quickly and without much negotiation.

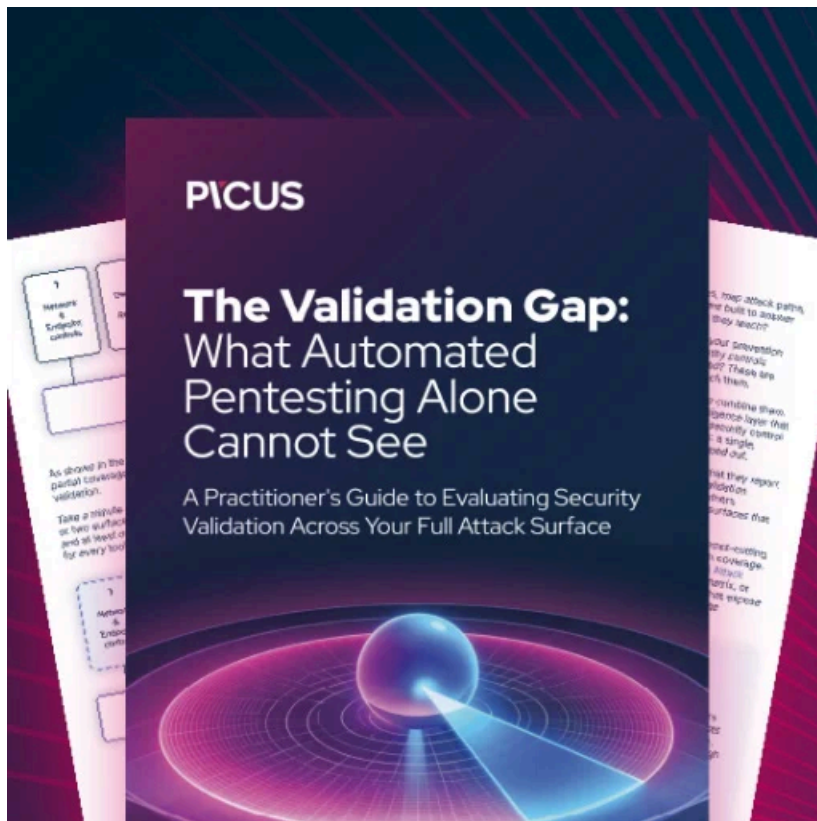
Some of the most notable recent incidents against firms in the industry include:

- [A.P. Møller-Maersk](#) hit by NotPetya ransomware in January 2018
- [COSCO](#) hit by an undetermined group of ransomware actors in July 2018
- [Pitney Bowes](#) hit by an undetermined group of ransomware actors in October 2019
- [U.S. Coast Guard](#) hit by Ryuk ransomware in December 2019

At this time, the shipping industry is going through a turbulent period, struggling to keep up with pressing demand in the post-pandemic world.

The cost of shipments has tripled since 2019, delivery delays are still on the rise, shortages and inflation are growing, and all contracts are under renegotiation.

It's a "perfect storm" for the industry, and ransomware actors likely see it as an excellent opportunity for successful extortions.



### [Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.