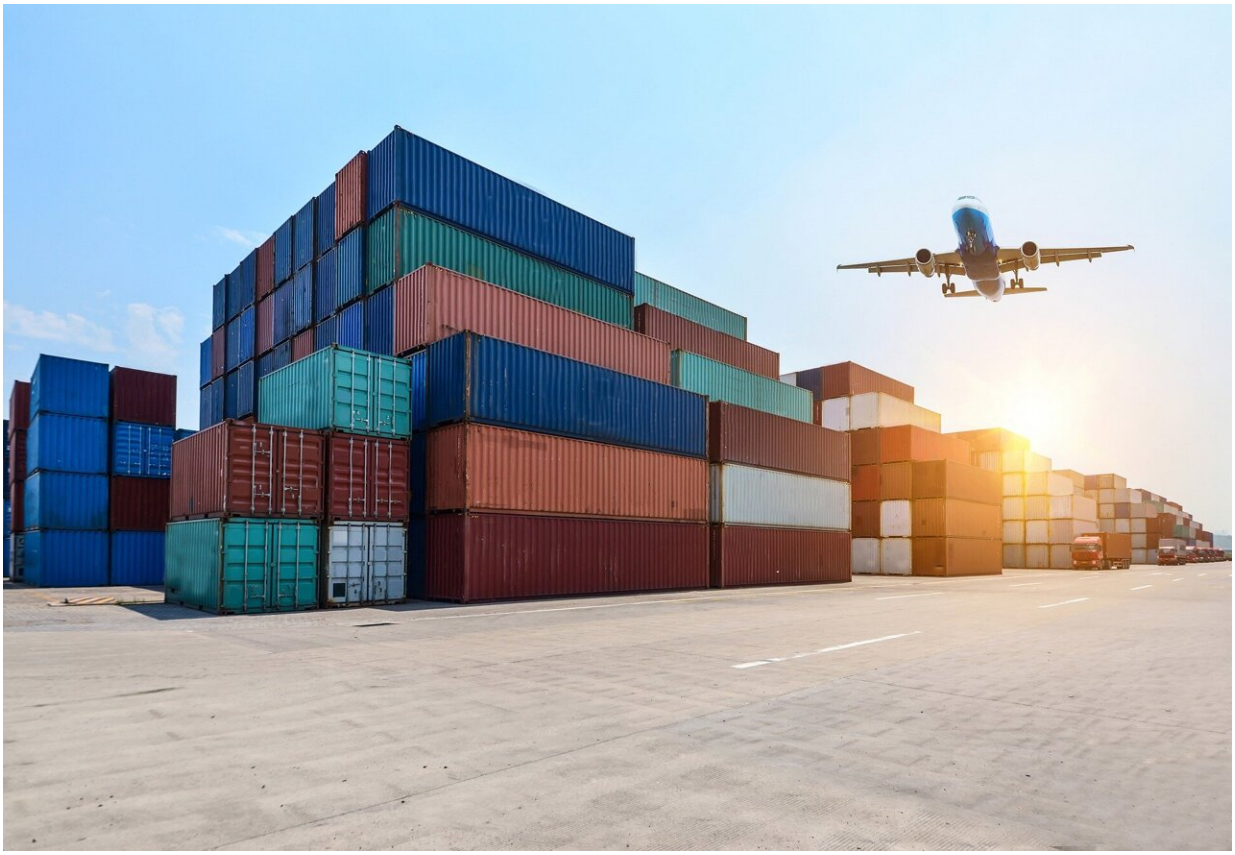
Major cyberattack on Australian ports suggests sabotage by a 'foreign state actor'

November 13 2023, by David Tuffley



Credit: Pixabay/CC0 Public Domain

A serious cyberattack has disrupted operations at several of Australia's largest ports, causing delays and congestion. Late on Friday, port operator DP World detected an IT breach that affected critical systems

used to coordinate shipping activity.

DP World is one of Australia's largest port operators, handling approximately 40% of the nation's container trade across terminals in Brisbane, Sydney, Melbourne and Fremantle.

DP World reacted quickly to contain the breach, including shutting down access to their port networks on land, to prevent further unauthorized access. This means they essentially "pulled the plug" on their internet connection to limit possible further harm.

DP World senior director Blake Tierney said it is still possible to unload containers from ships, but the trucks that transport the containers cannot drive in or out of the terminals. This is a precaution when the full extent of a data breach is not known.

The latest media reports suggest cargo could be stranded at the ports for several days.

Australian Federal Police and the Australian Cyber Security Centre are investigating the source and nature of the attack, deemed a "nationally significant incident" by federal cybersecurity coordinator Darren Goldie.

Is there evidence of this being a malicious attack?

The timing, scale and impact of the disruption do suggest this was a targeted attack.

It occurred on a Friday night, when most staff were off duty and less likely to notice or respond to the incident. The target was a major port operator that handles a significant share of Australia's trade and commerce. Such an attack can have serious consequences for Australia's economy, security and sovereignty.

The identity and motive of the attackers are not yet known, but the skills needed to mount such an attack suggest a foreign state actor trying to undermine Australia's national security or economic interests.

In recent years, cyberattacks on ports and shipping have become more common. For instance, in February 2022, several European ports were hit by a cyberattack that disrupted oil terminals. In another incident early this year, a ransomware attack on maritime software impacted more than 1,000 ships. Also in January 2023, the Port of Lisbon was targeted by a ransomware attack which threatened the release of port data.

These incidents highlight the vulnerability of the maritime industry to cyber threats and the need for increased cybersecurity measures.

How might the attack have happened?

So far, the details have not been disclosed. But based on what we know about similar cases, it is possible the attack took advantage of vulnerabilities in DP World's system. These vulnerabilities are normally closed by applying a "patch" in the same way your browser needs updating every week or two to keep it safe from being hacked.

Once hackers gained access, the breach likely pivoted to infiltrate the operational systems that directly manage port activities. Failing to isolate and secure these control networks allowed the incident to impact operations.

It is also possible access was gained via a phishing email or a malicious link. Such an attack may have tricked an employee or a contractor into opening an attachment or clicking on a link that installed malware or ransomware on the network.

Now what?

DP World is working urgently to rebuild affected systems from backups. However, resetting port management networks is a complicated process that could take days or weeks. Until the operator's core systems are securely restored, cargo flows may face ongoing delays.

The Australian government is closely involved in managing the situation, providing support and advice to DP World and other affected parties through the Critical Infrastructure Centre and the Trusted Information Sharing Network. These government agencies are equipped to provide timely support in times of crisis.

How can we prevent future attacks?

The DP World cyberattack is a clear warning of the risks to the essential transportation services that power Australia's trade and commerce.

Ports are difficult targets. To cause such a disruption, the attackers would have to be highly skilled and plan ahead. The fact ports have been successfully hacked more than once in recent times suggests threats from cybercriminals are steadily increasing.

For companies such as DP World, it's important to continuously monitor networks in real time, promptly install security updates and keep critical systems separated from each other.

Dedicated, well-resourced cybersecurity personnel, employee training and incident response plans are key to improving preparedness.

Ports should closely coordinate with government counterparts and industry partners on intelligence sharing and cybersecurity best practices.

Cyberthreats evolve so quickly, always being prepared for the latest one is a significant challenge.

For a seamless flow of goods, we need to be constantly vigilant of potential threats to our supply chain infrastructure. This latest attack is an urgent reminder that cyber resilience must be a top priority.

Provided by The Conversation