Port of Lisbon website still down as LockBit gang claims cyberattack

By Jonathan Greig

Published: 2023-02-02 · Archived: 2026-04-05 18:13:39 UTC

The website for the Port of Lisbon is still down days after officials confirmed it was the target of a cyberattack.

The Port of Lisbon is Portugal's busiest and one of the most used across all of Europe, handling 13,200,000 tonnes of cargo each year due to its strategic location between Europe and Africa.

On Christmas Day, officials with the Administration of the Port of Lisbon (APL) told the newspaper Publico that it had been targeted. Despite the attack, port officials said the incident did not compromise operational activity but noted that both the National Cybersecurity Center and the Judiciary Police were notified of the incident.

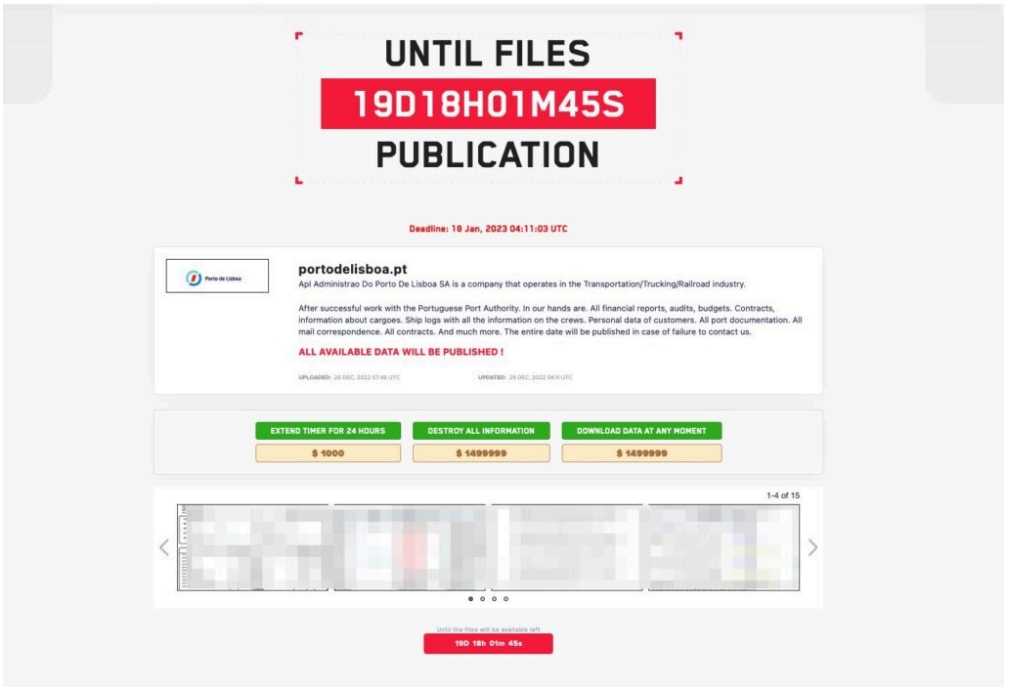
“All security protocols and response measures planned for this type of occurrence were quickly activated,” port officials told Publico in a statement.

"The Administration of the Port of Lisbon (APL) is working permanently and closely with all the competent authorities, in order to guarantee the security of the systems and respective data.”

The organization did not respond to repeated requests for comment and as of Thursday afternoon, its website was still unresponsive.

On Thursday, the LockBit ransomware group said it launched the attack against the port, claiming to have stolen financial reports, audits, budgets, contracts, ship logs and other information about cargo and crews.

The gang gave the port until January 18 to comply with ransom demands, threatening to leak the stolen data.



The attack is the latest in a series of cyberattacks on ports across Europe that have caused massive issues. In February, European prosecutors and cybersecurity officials began investigating a ransomware attack affecting several major oil port terminals.

Oil companies Oiltanking and Mabanaft, both owned by German logistics conglomerate Marquard & Bahls, suffered a cyberattack that crippled their loading and unloading systems in February. Oiltanking said it “declared force majeure” due to the attacks.

The attacks forced Shell to reroute oil supplies to other depots. German newspaper Handelsblatt said 233 gas stations across Germany had to run some processes manually because of the attack.

Last month, Secretary of the U.S. Department of Homeland Security Alejandro Mayorkas told Congress that the most significant threat to U.S. ports are cyberattacks.

"We are increasing the level of technology by which our ports operate and that is why not only Customs and Border Protection have a focus on cybersecurity but so does the United States Coast Guard,” Mayorkas said.

“I would identify, with respect to our ports, cybersecurity, as a significant threat stream and we are of course very focused on defending against it and strengthening our cybersecurity.”

Several cybersecurity experts said ports are ripe targets for cybercriminals and nation-states interested in causing disruption and harm.

Chris Grove, a director at cybersecurity firm Nozomi Networks, told The Record that disrupting port operations can have cascading impacts into other sectors, similar to attacks on power infrastructure.

“For example, China is heavily reliant on their ports to feed their energy backbone, most of their power generation comes from imported-by-sea coal and oil,” he said.

“Any disruption to that flow, ranging from a naval blockade to a cyberattack, could be crippling to any nation. Having that powerful capability in the hands of criminal ransomware operators should cause concern for those responsible for public safety and security.”

Ports and maritime operations have unique attributes that are attractive to threats: global footprint, high frequency of contact, and an amplified impact of loss all make a cyberattack a critical consideration, according to SynSaber co-founder Ron Fabela.

During the NotPetya attack in 2017 it became apparent that ports do not need to be specifically targeted in order to be impacted, he explained, noting that Maersk reported losses of up to $300 million dollars.

Grant Geyer, chief product officer at Claroty, echoed that assessment, explaining that the Russian NotPetya worm paralyzed supply chains by locking up ports and shipping companies worldwide – costing billions of dollars in direct and collateral damage.

With aging infrastructure, IT and OT systems in ports represent a prime target for cyber criminals to extract a payment for ransomware attacks, Geyer said, adding that for foreign adversaries, a cyberattack against a port creates an opportunity to project power by taking down supply chains and seize up an economy without using bombs or bullets.

“For industrial control systems, specifically ports and maritime, drive-by ransomware events will continue as we move into 2023. The impact of a cyberattack on ports has a downstream effect on numerous critical infrastructure and way of life for people,” Fabela said.

No previous article

No new articles

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.
