US Coast Guard discloses Ryuk ransomware infection at maritime facility

By Written by Catalin Cimpanu, ContributorContributor Dec. 29, 2019 at 10:00 p.m. PT

Archived: 2026-04-05 19:10:44 UTC

See als

-

An infection with the Ryuk ransomware took down a maritime facility for more than 30 hours; the US Coast Guard said in a security bulletin it published before Christmas.

The agency did not reveal the name or the location of the port authority; however, it described the incident as recent.

"Forensic analysis is currently ongoing but the virus, identified as 'Ryuk' ransomware," the US Coast Guard (USCG) said in a security bulletin meant to put other port authorities on alert about future attacks.

Point of entry: phishing email

USCG officials said they believe the point of entry was a malicious email sent to one of the maritime facility's employees.

"Once the embedded malicious link in the email was clicked by an employee, the ransomware allowed for a threat actor to access significant enterprise Information Technology (IT) network files, and encrypt them, preventing the facility's access to critical files," the agency said.

The USCG security bulletin describes a nightmare scenario after this point, with the virus spreading through the facility's IT network, and even impacting "industrial control systems that monitor and control cargo transfer and encrypted files critical to process operations."

Coast Guard officials said the Ryuk infection caused "a disruption of the entire corporate IT network (beyond the footprint of the facility), disruption of camera and physical access control systems, and loss of critical process control monitoring systems."

The maritime facility -- believed to be a port authority -- was forced to shut down its entire operations for more than 30 hours, the Coast Guard said.

Increase in maritime cyber threats

The agency's security bulletin includes basic advice for preventing infections with the Ryuk ransomware. The Coast Guard published the advisory on December 16 in an attempt to broadcast the event to as many maritime facilities as fast as possible and get them to deploy countermeasures before they were targeted as well.

The alert does not detail a novel threat. Port authorities and ships have long been considered easy to hack, and ransomware gangs have targeted ports in the past.

In July 2018, there was a ransomware attack that was initially reported as an infection affecting the Long Beach Port. The infection was later tracked down and isolated to the port terminal of the China Ocean Shipping Company (COSCO), one of the largest shipping companies in the world.

In September 2018, the ports of San Diego (US) and the port of Barcelona (Spain) reported ransomware infections within five days of each other. Both incidents were later revealed to have been caused by the same Ryuk ransomware.

A report published in December 2018 by a conglomerate of 21 international shipping associations and industry groups highlighted an increase in cyber-security problems aboard ships and in ports, where investigators found ransomware, USB malware, and worms, on numerous occasions.

This rise in cybersecurity threats to ships and ports has pushed the US Coast Guard to take notice and act accordingly. Starting this year, the US Coast Goard has begun issuing security alerts for cybersecurity-related threats, and not only for physical damage, terrorism, or piracy issues.

This latest security bulletin is the third such alert the USCG sent out this year after sending the first two in May and July. These first two alerts were about malware designed to impact IT systems found aboard ships, rather than a maritime facility.

The FBI's most wanted cybercriminals

Security
