The Port of San Diego has suffered a ransomware cyber attack affecting its IT systems, and federal law enforcement is investigating the assault. The port says that the attack has affected its administrative functions related to port permits, public records requests, and business services, but that it has not interfered with maritime operations. The FBI and the Department of Homeland Security are involved in investigating the attack.

"The Port remains open, public safety operations are ongoing, and ships and boats continue to access the Bay without impacts from the cybersecurity incident," said Port CEO Randy Coniglio in an updated Thursday.

The cybersecurity involves the use of ransomware, as seen previously in the "NotPetya" attack on Maersk and APMT Terminals last year. Coniglio said that the ransom demand for restoring service involves a payment in Bitcoin, as is typical for ransomware attacks.

The port did not disclose the amount demanded for the ransom, but it is said to be large. In recent infections with the "Bad Rabbit" ransomware package, the ransom amount has been set at up to 35 Bitcoin (about $230,000), according to IT industry sources.

Some ransomware packages are available as a service for enterprises, hackers, and other entities for a fee. Port operations have been affected in recent years by ransomware attacks, including in May 2017. The WannaCry ransomware worm hit the Port of San Diego and disrupted operations. The WannaCry ransomware worm hit Global Maritime Executive (GME) and Ryuk ransomware attacks have also been linked with North Korean hackers.

The U.S. Department of Justice has formally charged a member of North Korea’s notorious Lazarus Group in connection with the WannaCry ransomware outbreak. The U.S. Department of Justice has formally charged a member of North Korea’s notorious Lazarus Group in connection with the WannaCry ransomware outbreak. The U.S. Department of Justice has formally charged a member of North Korea’s notorious Lazarus Group in connection with the WannaCry ransomware outbreak.

Second port cyberattack in two weeks

A separate, unrelated attack hit the Port of Baltimore, Spain last week, and local media reported that it had an effect on cargo operations. The port warned on September 20 that delivery and reception of goods could be somewhat delayed. However, on Saturday, the port authority said that the attack had no effect on "normal seaport operations." The FBI and the Department of Homeland Security are involved in investigating the attack.

The Port of San Diego has suffered a ransomware cyber attack affecting its IT systems, and federal law enforcement is investigating the assault. The port says that the attack has affected its administrative functions related to port permits, public records requests, and business services, but that it has not interfered with maritime operations. The FBI and the Department of Homeland Security are involved in investigating the attack.

"The Port remains open, public safety operations are ongoing, and ships and boats continue to access the Bay without impacts from the cybersecurity incident," said Port CEO Randy Coniglio in an updated Thursday.

The cybersecurity involves the use of ransomware, as seen previously in the "NotPetya" attack on Maersk and APMT Terminals last year. Coniglio said that the ransom demand for restoring service involves a payment in Bitcoin, as is typical for ransomware attacks.

The port did not disclose the amount demanded for the ransom, but it is said to be large. In recent infections with the "Bad Rabbit" ransomware package, the ransom amount has been set at up to 35 Bitcoin (about $230,000), according to IT industry sources.

Some ransomware packages are available as a service for enterprises, hackers, and other entities for a fee. Port operations have been affected in recent years by ransomware attacks, including in May 2017. The WannaCry ransomware worm hit the Port of San Diego and disrupted operations. The WannaCry ransomware worm hit Global Maritime Executive (GME) and Ryuk ransomware attacks have also been linked with North Korean hackers.

The U.S. Department of Justice has formally charged a member of North Korea’s notorious Lazarus Group in connection with the WannaCry ransomware outbreak. The U.S. Department of Justice has formally charged a member of North Korea’s notorious Lazarus Group in connection with the WannaCry ransomware outbreak. The U.S. Department of Justice has formally charged a member of North Korea’s notorious Lazarus Group in connection with the WannaCry ransomware outbreak.

Second port cyberattack in two weeks

A separate, unrelated attack hit the Port of Baltimore, Spain last week, and local media reported that it had an effect on cargo operations. The port warned on September 20 that delivery and reception of goods could be somewhat delayed. However, on Saturday, the port authority said that the attack had no effect on "normal seaport operations." The FBI and the Department of Homeland Security are involved in investigating the attack.