Shipping giant COSCO brutalized by ransomware attack

Derek Kortepeter

August 3, 2018

Reports from multiple news sources, as well as from COSCO itself, are showing that the major shipping company has succumbed to a ransomware attack. In a company statement released on Facebook (due to the website still being down at the time of this article’s writing), COSCO (China Ocean Shipping Co.) had this to say:

Due to the local network breakdown within our Americas region, local email and network telephone is not working properly at the moment. For safety precautions, we have shut down connections with other regions for further investigations.

So far, all vessels of our company are operating normally, and our main business operation systems are stable. We are glad to inform you that we have taken effective measures and aside from the Americas region, the business operation within all other regions will be recovered very soon. The business operations in the Americas are still being carried out, and we are trying our best to make a full and quick recovery. We will keep you updated of the latest progress through various channels.

There is more to the story though, as the maritime news site Lloyd’s List reports this was not a “network breakdown” but ransomware attack. Their sources for this information are internal emails from COSCO in which a ransomware attack is directly mentioned. Contents of the emails in question contained direct instructions such as telling employees “not to open ‘suspicious’ emails.” Additionally the company stated internally that they have “requested a computer inspection in China with anti-malware software.”

The investigation is ongoing, but as with all ransomware, it was likely caused by someone unknowingly executing files in an attachment or by clicking on a link that was malicious. The social engineering aspect of ransomware is what keeps the attack on the common list of hacking methods for cybercriminals. Somebody is always willing to take the bait in your phishing emails, and when they do, you can capitalize. It is not known, at the time of writing this article, what kind of ransomware COSCO came under attack from. Should the company further release information that pertains to this there may be a follow-up post on this issue.