UK rail network Merseyrail likely hit by Lockbit ransomware

bleepingcomputer.com/news/security/uk-rail-network-merseyrail-likely-hit-by-lockbit-ransomware/

Lawrence Abrams

By
Lawrence Abrams

- April 28, 2021
- 04:15 AM
- 0

UK rail network Merseyrail has confirmed a cyberattack after a ransomware gang used their email system to email employees and journalists about the attack.

Merseyrail is a UK rail network that provides train service through sixty-eight stations in the Liverpool City Region in England.

"We can confirm that Merseyrail was recently subject to a cyber-attack. A full investigation has been launched and is continuing. In the meantime, we have notified the relevant authorities," Merseyrail told BleepingComputer yesterday after we received a mysterious email earlier this month from the account of Andy Heath, the Director of Merseyrail.

Ransomware gang uses Merseyrail's email system against them

While the cyberattack has not been publicly disclosed, BleepingComputer learned of the attack after receiving a strange email on April 18th from Heith's email account with the mail subject, "Lockbit Ransomware Attack and Data Theft."

This email was sent to BleepingComputer, various UK newspapers, and the staff of Merseyrail in what appears to be a takeover of the Director's @merseyrail.org Office 365 email account by the Lockbit Ransomware gang.

In this email, the threat actors pretended to be Merseyrail's Director telling employees that a previous weekend's outage was downplayed and that they suffered a ransomware attack where the hackers stole employee and customer data.

Included in the email is a link to an image showing an employee's personal information that Lockbit allegedly stole during the attack.

After numerous attempts to contact Merseryrail and confirm the attack, we finally received the rail network's statement last night.

"It would be inappropriate for us to comment further while the investigation is underway," Merseyrail told BleepingComputer when we questioned how the Director's email was compromised.

In response to our queries, the UK Information Commissioner's Office (ICO) also confirmed that Merseyrail made them aware of the "incident."

"Merseyrail has made us aware of an incident and we are assessing the information provided," the ICO told BleepingComputer via email.

Ransomware gangs aggressively extort victims

Over the past year, ransomware gangs have become increasingly aggressive in their extortion tactics.

In the past, ransomware attacks consisted of threat actors stealing victims' data and then encrypting their files to force a ransom payment.

Over time, threat actor's tactics have escalated to performing DDoS attacks on victims' networks and websites, emailing customers and journalists, and threatening to contact stock exchanges.

Sadly, while these attacks are ongoing, the employees and customers are usually the last to know what is happening with their data and organization.

Using a victim's email system to promote their attacks to both employees, journalists, and customers could turn that on its head.

Related Articles:

Costa Rica declares national emergency after Conti ransomware attacks

The Week in Ransomware - May 6th 2022 - An evolving landscape

Conti, REvil, LockBit ransomware bugs exploited to block encryption

New Black Basta ransomware springs into action with a dozen breaches

American Dental Association hit by new Black Basta ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.