

LockBit ransomware gang claims Royal Mail cyberattack

By Sergiu Gatlan

Published: 2023-02-07 · Archived: 2026-04-05 15:08:03 UTC



The LockBit ransomware operation has claimed the cyberattack on UK's leading mail delivery service Royal Mail that forced the company to halt its international shipping services due to "severe service disruption."

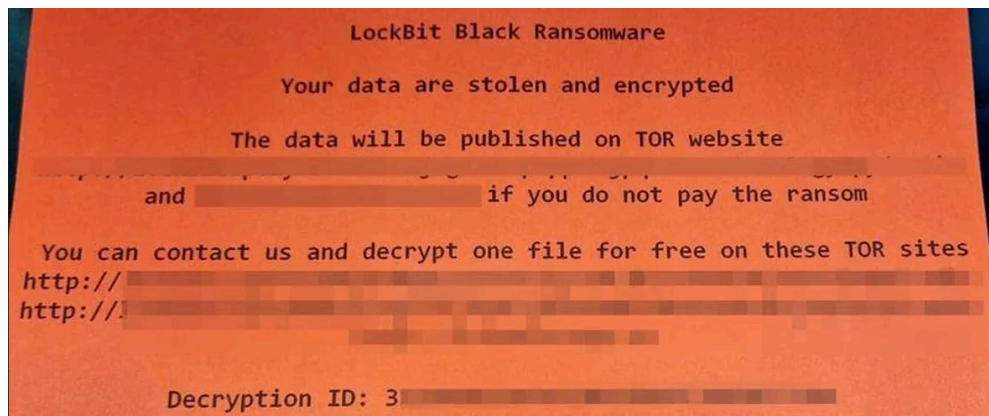
This comes after LockBitSupport, the ransomware gang public-facing representative, previously told BleepingComputer that [the LockBit cybercrime group did not attack Royal Mail](#).

Instead, they blamed the attack on other threat actors using the [LockBit 3.0 ransomware builder](#) that was leaked on Twitter in September 2022.



Visit Advertiser website [GO TO PAGE](#)

LockBitSupp failed to explain why printed Royal Mail ransom notes seen by BleepingComputer included links to LockBit's Tor negotiation and data leak sites rather than ones operated by another threat actor.



Lockbit Black ransom note printer during the attack on Royal Mail ([Daniel Card](#))

However, LockBitSupp confirmed that LockBit was indeed behind the attack in a post on a Russian-speaking hacking forum after determining that one of their affiliates deployed the gang's ransomware payloads on Royal Mail's systems.

The ransomware gang's representative also added that they would only provide a decryptor and delete data stolen from Royal Mail's network after a ransom is paid.

At the moment, the entry for the Royal Mail attack on LockBit's data leak site says stolen data will be published online on Thursday, February 9, at 03:42 AM UTC.



Royal Mail entry on LockBit's data leak site ([BleepingComputer](#))

Attack described as a "cyber incident"

Royal Mail [first detected the attack](#) on January 10 and hired outside forensic experts to help with the investigation.

"Incident was detected yesterday, UK/ domestic mail remains unaffected," a Royal Mail spokesperson told BleepingComputer on January 11 when we reached out for more details.

"We're experiencing disruption to our international export services and are temporarily unable to despatch items to overseas destinations," the company [tweeted](#).

"Please do not post any export items while we work to resolve the issue. Sorry for any disruption this may cause."

The company also reported the incident to UK security agencies and is investigating the incident alongside the National Crime Agency and UK National Cyber Security Centre (NCSC).

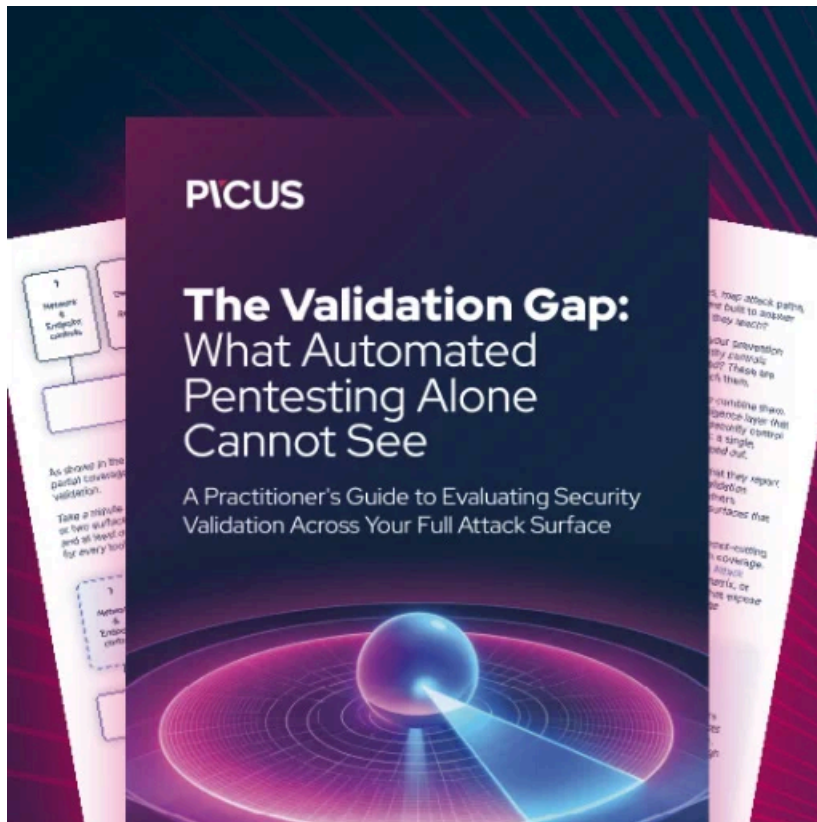
However, Royal Mail is yet to acknowledge that it's dealing with a ransomware attack that could likely lead to a data breach since LockBit ransomware operators are known for stealing data and leaking it online if their ransom demands are not met.

For now, the company is still describing the attack as a "cyber incident" and says that it has restored some of the services impacted by the attack.

Last month's incident follows a [November 2022 outage](#) that led to the Royal Mail's tracking services being unavailable for more than 24 hours.

Royal Mail's recurring IT issues come at a time when its mailing services are already strained amid [planned national strikes and ongoing negotiations with the Communication Workers Union](#).

H/T [Dominic Alvieri](#)



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-claims-royal-mail-cyberattack/>