Russian-linked ransomware gang behind Royal Mail cyber attack

A ransomware gang linked to Russia carried out the Royal Mail cyber attack that suspended international postal deliveries.

It is understood that Royal Mail's investigation found the gang, named Lockbit, infected machines that print customs labels for parcels being sent overseas. The **attack** has left more than half a million parcels and letters stuck in limbo.

Lockbit's signature ransomware, known as Lockbit Black, scrambles computer files and demands payment in cryptocurrencies that are hard to trace in exchange for unscrambling them.

The ransom note, seen by The Telegraph, says: "Lockbit Black Ransomware. Your data are [sic] stolen and encrypted.

"You can contact us and decrypt one file for free."

The gang also threatened to publish stolen data on the dark web.

Printers at a Northern Irish **Royal Mail** distribution centre reportedly began "spurting" out copies of the ransom note – a signature tactic of the gang.

More on Royal Mail

Royal Mail unable to despatch items abroad after ‘cyber incident’

Strikes and the unions: How have they changed?

Simon Thompson urges striking union to ‘think carefully about members’ jobs and saving Christmas’

Related Topics:

- Royal Mail

Staff at the centre in Mallusk, County Antrim, reported the incident on Tuesday, according to the Belfast Telegraph.

Royal Mail declined to comment, but said on Wednesday: “We have asked customers temporarily to stop submitting any export items into the network while we work hard to resolve the issue.”

The National Cyber Security Centre, a branch of GCHQ, is helping the postal service remove the malicious software.

The National Crime Agency has also started an investigation.

Lockbit is believed to have extorted an estimated £82m from previous victims, which have included children's hospitals and UK car dealership chain Pendragon.

The gang is also understood to have close links with Russia. A member of the cyber gang wrote in a blog post last year: "We benefit from the hostile attitude of the West (towards Russia). It allows us to conduct such an aggressive business and operate freely within the borders of the former Soviet (CIS) countries."

Russian authorities have been slow to act against ransomware suspects wanted internationally.

Just one alleged Lockbit member has been charged with taking part in cyber attacks – separate to the Royal Mail attack – by US authorities.

Mikhail Vasiliev, 33, from Ontario, Canada is alleged to have conspired to intentionally damage protected computers and send ransom demands, according to prosecutors.

The charges carry a maximum five-year prison sentence. Mr Vasiliev, a dual Russian-Canadian citizen, is currently awaiting extradition from Canada.

Royal Mail, one of the world's largest postal services, was still unable to send letters and parcels overseas on Thursday.