2023 Royal Mail ransomware

Royal Mail hit by Russia-linked ransomware attack

Severe disruption to Royal Mail's overseas deliveries has been caused by ransomware linked to Russian criminals, the BBC has been told.

The cyber-attack has affected the computer systems Royal Mail uses to despatch deliveries abroad.

Royal Mail has been warning customers since Wednesday of disruption due to a "cyber-incident".

Its latest advice is for people not to try to send international letters and parcels until the issue is resolved.

What is LockBit ransomware and how does it operate?

Name of malware and criminal group behind it, LockBit has been blamed for attack on Royal Mail

LockBit has emerged as the most prolific name in ransomware attacks and has now been blamed for an incident that has hit Royal Mail's international operations.

January 2023

2023 Royal Mail ransomware

Ransomware is malicious computer software that encrypts data and locks up systems.

The ransomware used in the attack is "Lockbit", according to a source close to the investigation.

Computer security firms say the software has been developed and used by criminal gangs with links to Russia.

The BBC has seen a ransom note sent by the criminals to Royal Mail which reads: "Your data are stolen and encrypted."

The ransom demand is expected to be in the millions, although sources close to the investigation say there are "workarounds" to get the system going again.

BBC website - 12 January 2023

What is ransomware?

Ransomware is a piece of malicious software, or malware, that is often inserted into an entity's computer network via a so-called "phishing attempt". This involves tricking the receiver into downloading the malware, commonly by clicking on a link or attachment contained in an email. The phishing attempt can also include trying to access the person's user name and password to get into the network, by fooling them into thinking they are logging on to the network in question.

The malware then encrypts infected computers, making it impossible to access their content. The rogue actor behind the attack then demands money from the affected entity - typically a company or government organisation - for those computers to be unlocked or decrypted. According to the US Treasury, US banks and financial institutions alone processed approximately $1.2bn (£990m) in ransomware payments in 2021.

The Guardian - 13 January 2023

Who is behind LockBit?

Most ransomware groups tend to operate from eastern Europe, former Soviet Republics and Russia itself. "LockBit falls into the same category," says Lewis. In November the US Department of Justice charged a dual Russian and Canadian national, Mikhail Vasiliev, over alleged participation in LockBit's ransomware campaign. The DoJ said LockBit had been deployed against at least 1,000 victims in the US and around the world, has made at least $100m in ransom demands and has "extracted tens of millions of dollars in actual ransom payments".

Victims of LockBit attacks include Pendragon, a UK car dealership company, which has refused to pay a $60m ransomware demand.

According to Trustwave, a US cybersecurity firm, the LockBit group "dominates the ransomware space" and uses large payments to recruit experienced actors. It accounted for 44% of ransomware attacks in January-September last year, according to Deep Instinct, an Israeli cybersecurity firm.

The malware was previously known as ".abcd", after the file extension that was added to encrypted files as they were made inaccessible. Ransomware, and the groups behind it, often undergoes name changes in order to avoid law enforcement or a company-style rebranding exercise after becoming excessively notorious.

The Guardian - 13 January 2023