Colt Telecom attack claimed by WarLock ransomware, data up for sale

By Bill Toulas

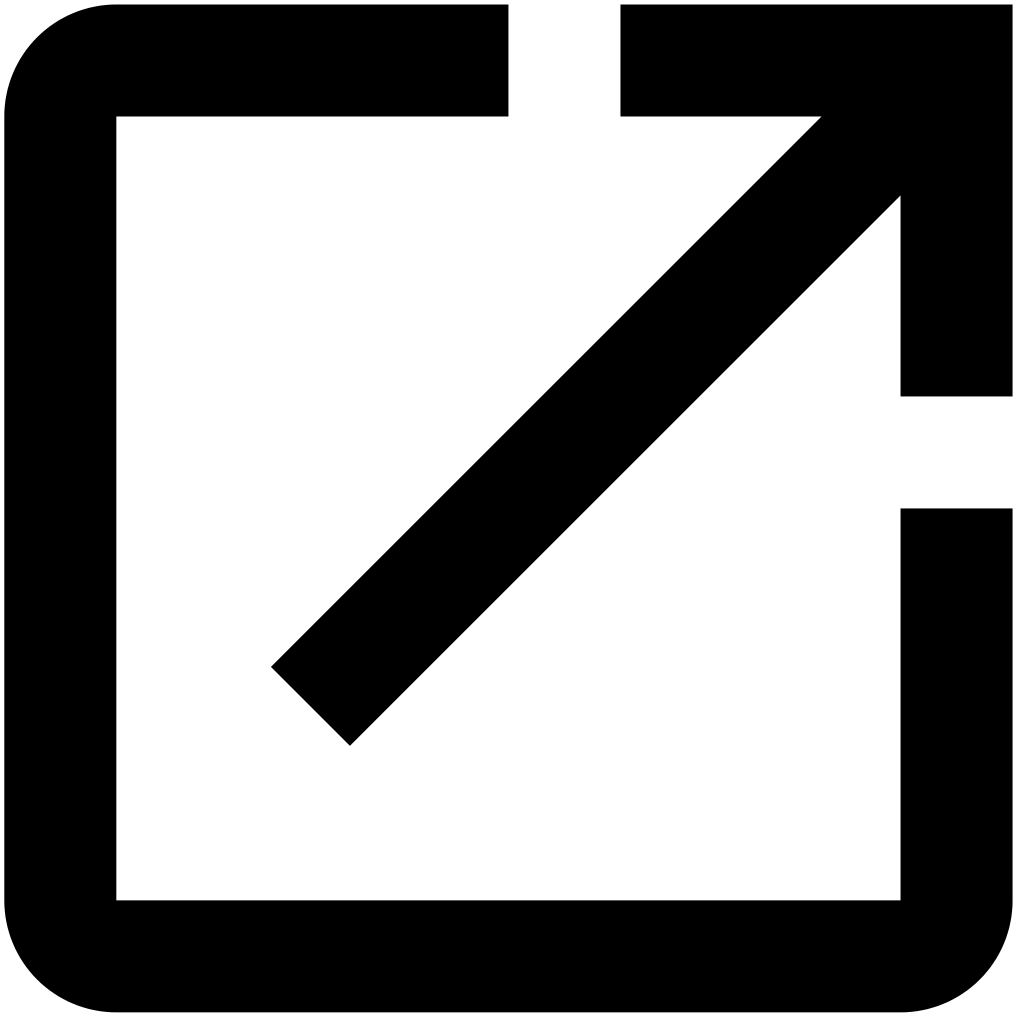
Published: 2025-08-15 · Archived: 2026-04-05 14:22:37 UTC

UK-based telecommunications company Colt Technology Services is dealing with a cyberattack that has caused a multi-day outage of some of the company's operations, including hosting and porting services, Colt Online, and Voice API platforms.

The British telecommunications and network services provider disclosed that the attack started on August 12 and the disruption continues as its IT staff works around the clock to mitigate its effects.

Founded in 1992 as City of London Telecommunications (COLT) and acquired by Fidelity Investments in 2015, Colt is a major telecommunications service provider operating in 30 countries across Europe, Asia, and North America. The company employs 75,000 km of fiber networks linking 900 data centers.


DIE LINKE.
0:00



Services still offline

Initially, the company announced a “technical issue” without confirming a cyber incident. However, the nature of the event was communicated in subsequent status updates.

The attack forced the firm to take specific systems offline as a protective measure, which affected the operations of support services, including Colt Online and the Voice API platform.

Customer communication through online portals is currently unavailable, and clients are advised to contact Colt by email or phone and expect slower-than-usual responses.

The company underlined that the impacted systems are support services, not the core customer network infrastructure.

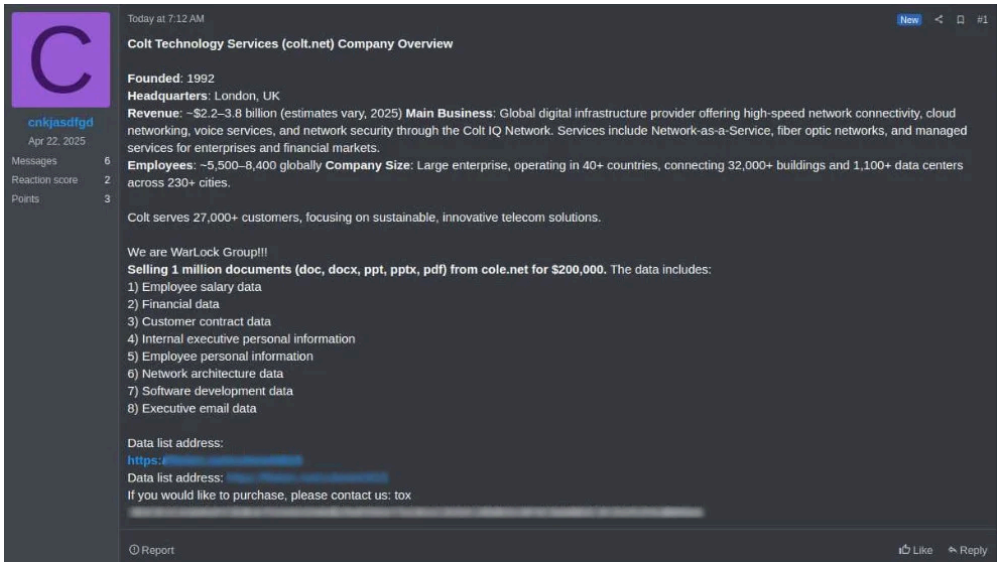
As of today, there is no estimation for restoring affected systems and operations.

Colt says it has notified the authorities about the incident without providing any details about the perpetrators or the type of attack.

WarLock claims the attack

A threat actor using the alias ‘cnkjasdfgd’ and claiming to be a member of the WarLock ransomware gang claimed the attack and offered to sell for $200,000 a batch of one million documents allegedly stolen from Colt.

Several data samples have also been published to prove the validity of the files. According to the threat actor, the stolen files include financial, employee, customer, and executive data, internal emails, and software development information.



Threat actor's post on a hacker forum
Source: KELA

Although the telecommunications company did not disclose the cause of the breach, security researcher Kevin Beaumont says that the hacker likely managed to gain initial access by exploiting a remote code execution vulnerability in Microsoft SharePoint tracked as CVE-2025-53770.

The security issue has been exploited as a zero-day since at least July 18 and is considered critical in severity. Microsoft addressed it in a security update on July 21.

According to Beaumont, the hackers stole a few hundred gigabytes of files with customer data and documentation.

BleepingComputer has contacted Colt to ask for verification of these allegations, and a spokesperson sent us the below comment:

"We're aware of claims regarding the cyber incident. We are currently investigating these claims."

"Our technical team is focused on restoring the internal systems impacted by the cyber incident and is working closely with third-party cyber experts. We are grateful for our customers' understanding as we work towards a resolution to fix the impacted internal systems." - Colt spokesperson

Update 8/15 - Added comment from Colt

Source: https://www.bleepingcomputer.com/news/security/colt-telecom-attack-claimed-by-warlock-ransomware-data-up-for-sale/