OpenVoiceNews

Transparent. Unbiased. Yours.

Colt Telecom Hit by Ransomware Attack as WarLock Hackers Claim Data Theft

August 18, 2025
— Categories: Defence & Security

© Bank Info Security

Colt Technology Services, one of the UK's leading telecommunications companies, has been hit by a major cyberattack claimed by the ransomware group WarLock. The incident, which has disrupted some customer-facing services, has raised fresh concerns about the vulnerability of telecom providers to sophisticated digital threats.

The company said it first detected a problem on 12 August when staff noticed faults affecting internal systems. What was initially treated as a technical fault was soon confirmed to be a cyberattack, prompting Colt to shut down key support platforms to prevent further spread. Among the services taken offline were the Colt Online customer portal and its Voice API platform, which are widely used by clients to manage networks and communications.

In a statement, Colt stressed that it was still able to monitor customer networks and respond to incidents, though the process had become slower as much of the work was now being done manually. The company urged customers to contact support teams directly via telephone or email while its digital platforms remained offline. “Our teams are working around the clock alongside cybersecurity experts to restore affected systems safely,” a spokesperson said.

The WarLock group has since claimed responsibility, boasting on underground forums that it has stolen up to one million files from Colt. The hackers are reportedly demanding $200,000 for the trove, which they claim contains financial records, emails, software development documents and customer data. To prove their claims, they released sample files online that appear to reference internal company materials, including staff performance reviews.

Cybersecurity analysts say the group may have exploited a recently discovered vulnerability in Microsoft SharePoint. The flaw, patched by Microsoft in July, allows attackers to remotely execute malicious code. Experts believe WarLock could have used this opening to gain access to Colt’s systems. Kevin Beaumont, an independent security researcher who reviewed some of the leaked data, said the material appeared authentic and warned that the threat actors may have obtained highly sensitive corporate information.

Colt has reported the breach to authorities and is now working with law enforcement and external cybersecurity specialists. While the company has not confirmed whether the data being circulated by WarLock is genuine, the scale of the claim has alarmed industry observers.

Ransomware attacks have become one of the most disruptive forms of cybercrime, targeting organisations across critical sectors from healthcare to energy. Telecommunications providers, which sit at the heart of modern infrastructure, are increasingly attractive targets because of their large data stores and reliance on complex networks.

This attack also highlights the risks companies face when patches and updates to widely used software are delayed or overlooked. Analysts argue that organisations must act quickly when new vulnerabilities are disclosed, as cybercriminals are swift to exploit any gaps.

For Colt's customers, the incident serves as a reminder of the importance of resilience. While the company works to restore services and assess the damage, its handling of the breach will be closely watched as a measure of its ability to safeguard client trust.

As investigations continue, Colt faces the difficult task of repairing both its systems and its reputation in the face of an attack that has once again underlined the escalating dangers of the cyber threat landscape.