Ransomware group may have stolen customer bank details from British water company

By Alexander Martin

Published: 2023-01-09 · Archived: 2026-04-06 00:29:27 UTC

South Staffordshire Water, which supplies water for more than 1.7 million people in England, has said that an attempted ransomware attack in August may have enabled cybercriminals to steal customer bank details.

At the time of the incident the company stressed that water supply was not affected, although its corporate network was experiencing disruptions. The company said in an update on Wednesday that customers who paid by direct debit may have had their bank details stolen.

“Since the incident, we’ve been working with leading forensic experts to investigate fully what happened. Our investigation has now found that the incident resulted in unauthorized access to some of the personal data we hold for a subset of our customers,” the company announced.

The affected details include the names and addresses associated with customers’ accounts as well as the bank details (account numbers and sort codes) used to set up direct debit payments. South Staffs said it is writing letters to the affected customers.

The company also said it had notified a number of regulatory bodies, including the National Crime Agency, National Cyber Security Centre, and the water services regulation authority Ofwat.

Water suppliers are required to report cybersecurity incidents to Ofwat under the U.K.’s Network and Information Systems (NIS) Regulations. However, the reporting obligation only applies to incidents which ultimately impact water supply, which the ransomware attack did not. The government announced yesterday it would update the legislation so that service providers would need to notify regulators “of a wider range of incidents.”

The attack on South Staffs Water was one of several ransomware incidents in the U.K. which have dominated recent Cabinet Office Briefing Rooms (COBR) meetings, bringing in officials from across government to assess the risks they pose to critical services.

The Cl0p ransomware group, which appears to be behind the attack, bungled its initial extortion attempt targeting South Staffs back in August when the hackers mistakenly claimed to have accessed a different water company’s network.

The group’s leak site also claimed that the hackers decided not to encrypt the company’s files and that they were demanding an extortion payment to prevent the release of stolen data and to disclose how they managed to access the company’s network.

Law firm Hayes Connor said it is currently working with 18 of the company’s employees “who have been affected by this data breach, with more clients expected to make a claim.”

“The information that we have received regarding the South Staffordshire Water data breach is very concerning. When a company of such large scale experiences a data breach, it means a significant amount of personal data is likely at serious risk of being misused,” said Richard Forrest, the firm’s legal director.

“When financial data is in jeopardy, individuals can fall victim to identity or takeover fraud. Criminals can then use this information to extract funds from the victim's bank account, as well as buy products and services, leading to both financial loss and emotional distress.”

No previous article

No new articles

Alexander Martin

is the UK Editor for Recorded Future News. He was previously a technology reporter for Sky News and a fellow at the European Cyber Conflict Research Initiative, now Virtual Routes. He can be reached securely using Signal on: AlexanderMartin.79
