Hackers attack UK water supplier but extort wrong company

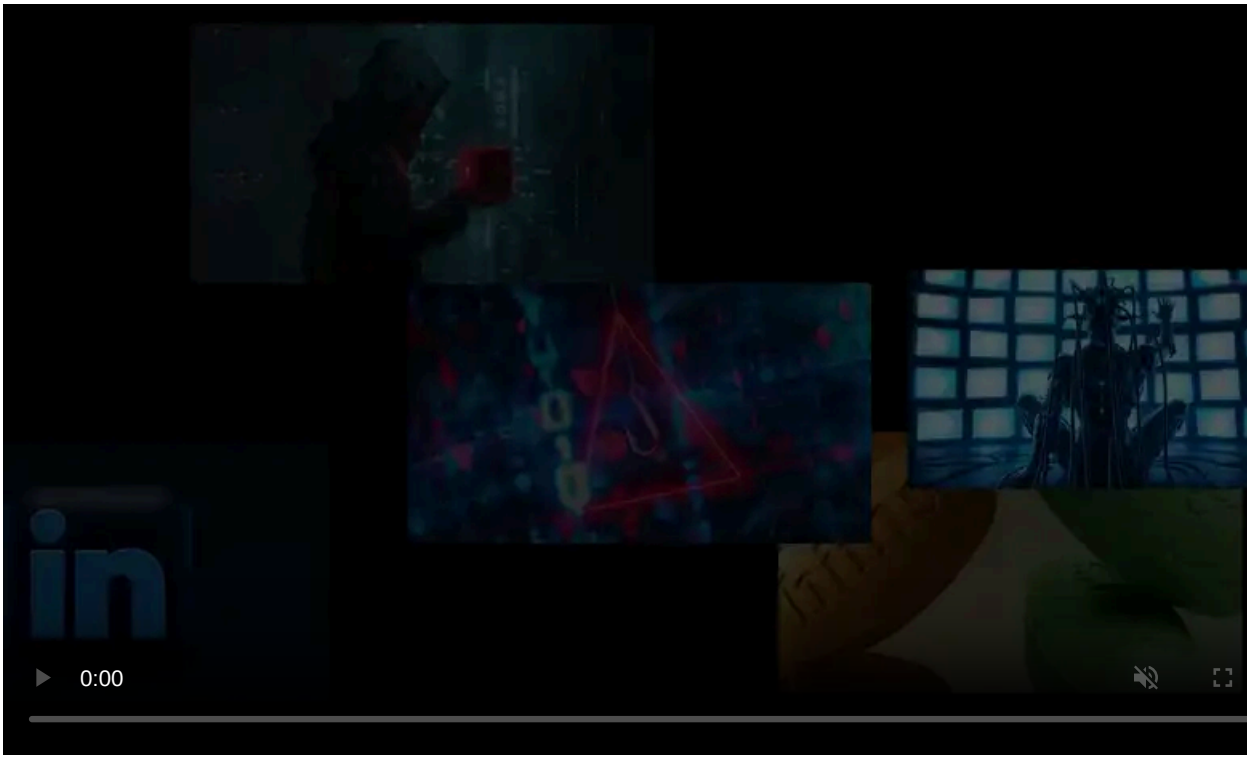
By Bill Toulas

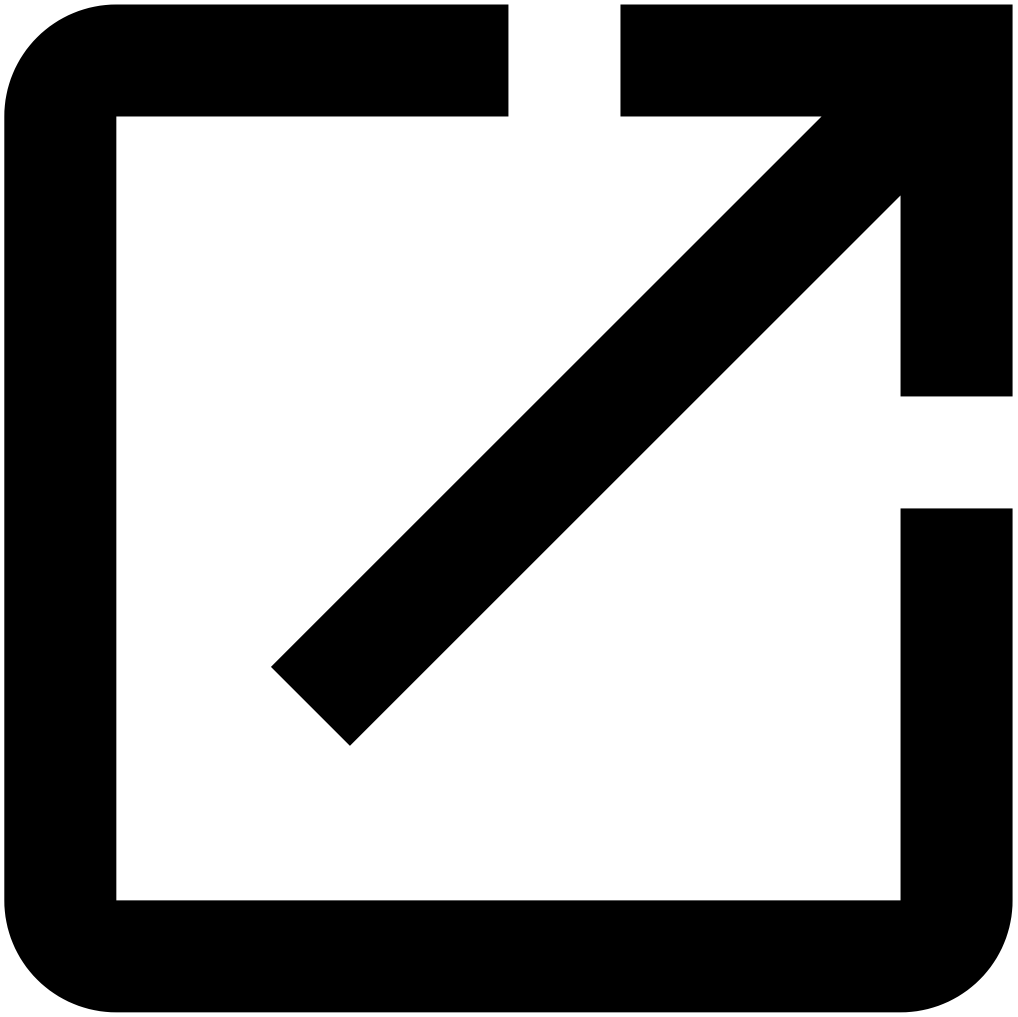
Published: 2022-08-16 · Archived: 2026-04-05 16:40:18 UTC

South Staffordshire Water, a company supplying 330 million liters of drinking water to 1.6m consumers daily, has issued a statement confirming IT disruption from a cyberattack.

As the announcement explains, the safety and water distribution systems are still operational, so the disruption of the IT systems doesn't impact the supply of safe water to its customers or those of its subsidiaries, Cambridge Water and South Staffs Water.

"This is thanks to the robust systems and controls over water supply and quality we have in place at all times, as well as the quick work of our teams to respond to this incident and implement the additional measures we have put in place on a precautionary basis," explains the statement published on the company's site.


0:00



Also, South Staffordshire Water reassures its customers that all service teams are operating as usual, so there's no risk of extended outages due to the cyberattack.

Clop misidentifies victim?

Meanwhile, the Clop ransomware gang claimed Thames Water as their victim via an announcement on their onion site today, alleging to have accessed SCADA systems they could manipulate to cause harm to 15 million customers.

Thames Water is UK's largest water supplier and wastewater treatment provider, serving Greater London and areas surrounding river Thames.

The hackers allege to have informed Thames Water of its network security inadequacies and claim that they acted responsibly by not encrypting their data and only exfiltrating 5TB from the compromised systems.

> Thames Water supply much of critical water services to people and companies. This company is public and this mean not only they bring water and sewage services to millions of people they also allow many people and company to invest with their stock offering. Companies like this have much responsibility and we contact them and tell them that they have very bad holes in their systems. ALL SYSTEMS.

> We spent months in the company system and saw first hand evidence of very bad practice. This company is all for money and not deliver reliable service. It is better to save one pound so management can make bonuses and stock price do well. They lost way when only concentration on finance.

> Clop is not political organization and we do not attack critical infrastructure or health organizations. We decide that we do not encrypt this company, but we show them that we have access to more of 5TB of data. Every system including SCADA and these system which control chemicals in water. If you are shocked it is good.

Part of Clop's claims in the gang's data leak extortion site

However, following a supposed collapse in the negotiations of the ransom payment, the actors published the first sample of stolen data that includes passports, screenshots from water treatment SCADA systems, driver's licenses, and more.

Thames Water has officially disputed these claims via a statement today, saying that reports of Clop having breached its network are "cyber-hoax" and that its operations are at full capacity.

One key detail in the case is that among the published evidence, Clop presents a spreadsheet with usernames and passwords, which features South Staff Water and South Staffordshire email addresses.

Published evidence pointing to SSW

Additionally, BleepingComputer observed, one of the leaked documents sent to the targeted firm is explicitly addressed to South Staffordshire PLC.

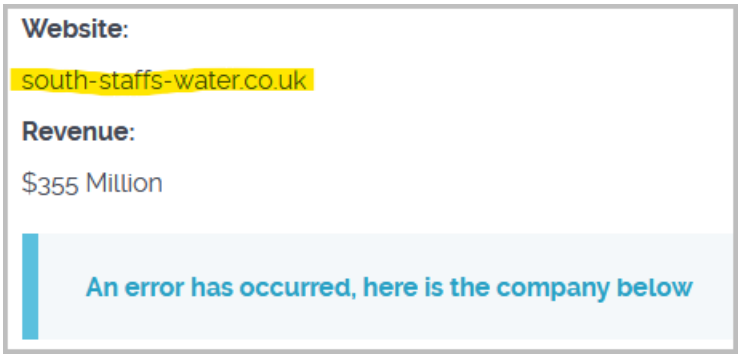
As such, it's very likely that Clop misidentified their victim or that they are attempting to extort a much larger company using false evidence.

This attack comes during dire drought times for UK consumers, with eight areas in the country imposing water ration policies and hosepipe bans.

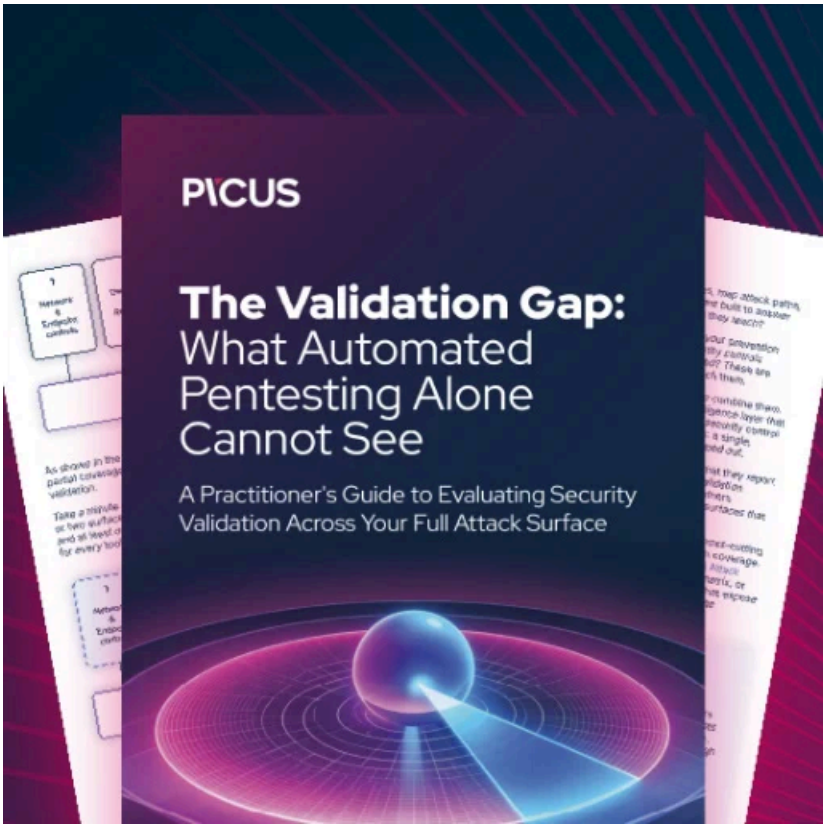
Cybercriminals don't pick their targets randomly, as hitting water suppliers during harsh drought periods could apply insurmountable pressure to pay the demanded ransom.

For this to happen, though, Clop has to redirect its threats to the correct entity, but considering the publicity the matter has taken, it's probably too late for that.

Update 8/17/22: Clop has corrected their error and now list South Staffordshire Water as the victim on the extortion site.



Listed victim on Clop site



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/hackers-attack-uk-water-supplier-but-extort-wrong-company/