

Capita Confirms Data Breach After Ransomware Group Offers to Sell Stolen Information

UK-based business process outsourcing and professional services company Capita has confirmed that hackers have stolen data from its systems after a well-known ransomware group offered to sell information allegedly stolen from the organization.

The incident came to light on March 31, when Capita said it was experiencing a major IT incident that prevented staff from logging into their systems. The company told the press at the time that it was too early to confirm that it was a cyberattack. However, information that came to light later showed that the company likely knew it was dealing with a cybersecurity incident.

Capita is one of the largest business outsourcing providers in the UK and its services are used by the country's government. A major data breach could have significant implications.

On April 3, Capita confirmed that it had experienced a cyber incident that prevented access to internal applications, which caused disruption to some services. The company said at the time that the "issue was limited to parts of the Capita network and there is no evidence of customer, supplier or colleague data having been compromised".

On April 8, the Black Basta ransomware group listed Capita on its leak website and shared some files as proof that they exfiltrated data from its systems. The leaked files stored personal and financial information and the hackers were

apparently hoping to find a buyer for the data rather than hoping that the victim would pay a ransom.

It took Capita until April 20 to confirm that some of its systems were in fact breached and that data had been stolen.

“From our investigations to date, it appears that the incident arose following initial unauthorised access on or around 22 March and was interrupted by Capita on 31 March,” the company said in a statement on Thursday. “As a result of the interruption, the incident was significantly restricted, potentially affecting around 4% of Capita’s server estate. There is currently some evidence of limited data exfiltration from the small proportion of affected server estate which might include customer, supplier or colleague data.”

The fact that Capita was dealing with a cyberattack on March 31 shows that the company likely knew about the nature of the incident, but refused to disclose it. It’s possible that the intrusion was discovered on March 31 because the attacker attempted to encrypt files on Capita systems.

Cybersecurity researcher Kevin Beaumont has criticized Capita for its attempt to downplay the incident to both the public and investors.

Beaumont reported that the data obtained by Black Basta included passport and driver’s license scans, payment details, floor plans for multiple buildings, employment screenings, and employment offer information.

The researcher pointed out that in a statement provided to the BBC this week the company still said it had no evidence of sensitive data being compromised. Beaumont learned that the company told the same thing to investors earlier this week.

Capita issued the statement confirming a data breach shortly after Beaumont announced plans to release a blog post detailing the hack.

Beaumont said Capita's systems were likely compromised as a result of a Qakbot email campaign launched on March 21 – in its latest statement the company confirmed being breached on March 22.

Qakbot, aka Qbot and Pinkslipbot, is a banking trojan that has been used by the Black Basta ransomware group to gain initial access to their targets.

Related: Ransomware Attack Hits Health Insurer Point32Health

Related: Payments Giant NCR Hit by Ransomware

Capita Confirms Data Breach After Ransomware Group Offers to Sell Stolen Information