# BA, Boots and BBC staff details targeted in Russia-linked cyber-attack

Publication Date: 2023-06-05

Author: Dan Milmo

Section: Technology

Tags: Cybercrime, Internet, British Airways, Boots, BBC, Retail industry, Russia, news

Article URL: https://www.theguardian.com/technology/2023/jun/05/ba-boots-and-bbc-staff-details-targeted-in-russian-linked-cyber-attack


British Airways, Boots and the BBC are investigating the potential theft of personal details of staff after the companies were hit by a cyber-attack attributed to a Russia-linked criminal gang. BA confirmed it was one of the companies affected by the hack, which targeted software called MOVEit used by Zellis, a payroll provider. “We have been informed that we are one of the companies impacted by Zellis’s cybersecurity incident, which occurred via one of their third-party suppliers called MOVEit,” said a spokesperson for the airline. An email sent to BA staff told employees that compromised information included names, addresses, national insurance numbers and banking details, according to the Daily Telegraph, which first reported the breach. BA said the hack had affected staff paid through BA payroll in the UK and Ireland. Boots said “some of our team members’ personal details” had been affected. The Telegraph reported that staff had been told that data involved in the attack included names, surnames, employee numbers, dates of birth, email addresses, the first lines of home addresses, and national insurance numbers. A BBC spokesperson also confirmed the broadcaster had been affected. The corporation believes the breach does not include staff bank details. “We are aware of a data breach at our third-party supplier, Zellis, and are working closely with them as they urgently investigate the extent of the breach. We take data security extremely seriously and are following the established reporting procedures,” the spokesperson said. Zellis said a “small” number of its customers had been hit by a vulnerability in MOVEit, a file transfer system used by the company. “We can confirm that a small number of our customers have been impacted by this global issue and we are actively working to support them,” it said, adding that the UK data watchdog and the National Cyber Security Centre had been informed. It is understood the attack has affected eight Zellis customers in the UK and Ireland. In a tweet on Sunday, Microsoft’s threat intelligence team attributed the attacks on MOVEit to a group it called Lace Tempest. It said the group was known for ransomware operations and running an “extortion site” carrying data extracted from attacks using a strain of ransomware known as Clop. Microsoft added: “The threat actor has used similar vulnerabilities in the past to steal data and extort victims.” Rafe Pilling, a director for threat research at the US cybersecurity firm Secureworks, said the attack was likely to have been carried out by an affiliate of the cybercriminal gang behind Clop ransomware, as well as the related website – referred to by Microsoft – where stolen data is advertised. Pilling said the entity behind Clop was a Russian-speaking cybercrime group. Pilling added that victims of the hack should expect to be contacted and asked for money for the return of any stolen data. “Victims will be contacted and if they refuse they will probably be listed and published on the Clop site,” he said. A spokesperson for MOVEit, which was developed by US firm Progress Software, said it had “corrected” the

vulnerability exploited by the hackers. “We are continuing to work with industry-leading cybersecurity experts to investigate the issue and ensure we take all appropriate response measures,” they said.