# BA, Boots and BBC cyber-attack: who is behind it and what happens next?

Publication Date: 2023-06-07

Author: Dan Milmo

Section: Technology

Tags: Cybercrime, Data and computer security, Internet, Russia, Boots, British Airways, BBC, explainers

Article URL: https://www.theguardian.com/technology/2023/jun/07/ba-boots-bbc-cyber-attack-moveit-who-is-behind-it-and-what-happens-next

British Airways, Boots and the BBC have been hit with an ultimatum to begin ransom negotiations from a cybercrime group after employees' personal data was stolen in a hacking attack. It emerged on Wednesday the gang behind a piece of ransomware known as Clop had posted the demand to its darkweb site, where stolen data is typically released if payments are not made by the victims. The group, who signed their darkweb message "friendly clop", exploited a piece of business infrastructure called MOVEit, software used to securely transfer files around internal networks, to attack the organisations. Who is behind the attack? Microsoft has attributed the attack to a group it calls Lace Tempest. The group is known for deploying a strain of ransomware called Clop, and an associated website where it displays its spoils and where it posts stolen details of victims who didn't pay. Secureworks, a US cybersecurity firm, said the people behind Clop are Russian-speaking and possibly based in Russia or members of the Commonwealth of Independent States (CIS) – the grouping of former members of the USSR that includes Belarus, Kazakhstan and Moldova. "It's a Russian-speaking organised cybercrime gang, not necessarily all based in Russia, although likely to be in Russia or CIS countries," said Rafe Pilling, a director for threat research at Secureworks. What is the gang demanding? In a message in broken English posted on the Clop darkweb site addressed "Dear Companies", it said that for companies who use MOVEit "chance is that we download alot of your data as part of exceptional exploit". It goes on to ask that users of MOVEit software contact the group via a pair of provided email addresses, which will prompt the sending of a chat URL that will be used – over an anonymised browser network – to start negotiations. The deadline for doing this is 14 June, they say, or else "we will post your name on this page". The group indicates that non-compliant hack victims will start to have their data published around 21 June, stating that "after 7 days all you data will start to be publication". If an organisation gets in touch they will be shown proof the gang has their data and they will have three days to "discuss price" for deleting that data. The message does not contain a price list or a means of payment. How did the attack happen? This was not a conventional ransomware attack, where a gang accesses a victim's IT networks, effectively locks up their computers via a piece of malicious code and then demands payment to restore access or delete/hand back data stolen during the attack. Instead, this was an attack that exploited a previously unknown flaw in MOVEit and allowed the gang to extract data undetected, without locking up the victims' networks. Such a flaw is known as a zero-day vulnerability, because of the lack of time between discovery of the weakness and its exploitation by attackers. According to Secureworks, the MOVEit attack appears to have been carried out by a dedicated team within the group, specialised in secure file transfers. Similar attacks on file transfer infrastructure have been linked to the group. Not every

victim was a direct user of MOVEit. One of the affected companies was Zellis, which provides outsourced payroll services to third parties. As a result, many Zellis customers had their employees' personal data being stolen in the attack. Should the victims pay? The British and US governments strongly advise against paying cyber ransoms. Last year the UK's data watchdog and National Cyber Security Centre wrote to legal professionals in England and Wales stressing that law enforcement did "not encourage" the payment of ransoms although payments were not usually unlawful. It is illegal to pay ransoms if the affected entity knows, or has reason to suspect, the proceeds will be used to fund terrorism. In the US, payment of ransoms is discouraged by the government, but an advisory note from the US Treasury in 2020 emphasised this was "explanatory only" and did "not have the force of law". Unlike conventional ransomware attacks, where victims are able to verify whether they have restored access to data after paying the ransom, for "hack and leak" attacks, those who do pay the ransom have to take it on trust their attacker has deleted the data as promised. In its ransom note to victims, Clop promises not to betray them any further. "Our team has been around for many years. We have not even one time not do as we promise. When we say data is delete it is cause we show video proof. We have no use for few measle dollars to deceive you." What should affected individuals do? "Given the detail of the leaked information, even including banking details, fraud is one of the biggest risks to affected customers right now," said Nick Guite of the cybersecurity experts SysGroup. "This information is often sold on the darkweb or in databases to criminal groups. They can then use it for identity theft, cloning or malicious phishing attacks to gain even more personal information. "If your company uses Zellis or has in any way been impacted by this breach, I'd highly recommend contacting an expert. Also, updating passwords and being vigilant for unexpected emails or phone calls will be important."