Cybercrime gang hits BA, Boots and BBC with ultimatum after mass hack

Publication Date: 2023-06-07

Author: Alex Hern

Section: Technology

Tags: Cybercrime, Hacking, BBC, British Airways, Boots, news

Article URL: https://www.theguardian.com/technology/2023/jun/07/cybercrime-clop-ultimatum-british-airways-boots--bbc-mass-hack

British Airways, Boots and the BBC have been hit with an ultimatum from the Russian-speaking cybercrime group Clop to begin ransom negotiations after it stole personal details of more than 100,000 staff across the organisations. The demand, posted on Clop's darkweb site, commands the affected companies to email the group by 14 June, or face having their stolen data posted online, which it is feared includes names, addresses, national insurance numbers and bank details. Clop exploited a piece of business infrastructure called MOVEit, software used to securely transfer files around internal networks, to attack the organisations. The same vulnerability provided an entry point into multiple victims in a single mass hack. Six organisations have confirmed to being affected, with Aer Lingus and the University of Rochester also admitting they have been hit. Many of the organisations are not direct users of the MOVEit software, but outsourced their payroll services to a third-party called Zellis, which was also hit. The hacker group claims to have information on "hundreds" of companies. In the post, they are coy about the nature of their attack, describing it merely as "penetration testing service after the fact". "This is announcement to educate companies who use Progress MOVEit product that chance is that we download a lot of your data as part of exceptional exploit," the demand reads. "We are the only one who perform such attack and relax because your data is safe." The ultimatum contains no explicit sum for businesses to pay, but demands that they enter into negotiations. The group also claims that it has deleted data that it may have stolen from state actors. "Do not worry, we erased your data you do not need to contact us," it says. "We have no interest to expose such information." Such olive branches are common from professional hacking groups, who want to maximise their income without bringing unnecessary attention from law enforcement. The threat is an escalation of conventional ransomware attacks and is known as "doxware". Rather than simply encrypting data and charging for a key, hackers steal the data directly and threaten to publish it unless the ransom is paid. While more technically challenging for the hackers, doxware prevents businesses from simply restoring their data from backups and ignoring ransom demands. "The attackers have chosen to ask their victims to begin negotiation tactics by reaching out initially but this approach deviates from the norm as typically ransom demands are sent to the targeted organisations with a predetermined amount chosen by the hackers," said Jake Moore, global cyber-security adviser at Eset. "This decision is likely to stem from the overwhelming magnitude of the ongoing hack which is still affecting large numbers of systems worldwide and potentially overpowering the capabilities of Clop itself. "Although it is never advised to pay ransom demands to cybercriminals, there is an inevitable risk that some of the targeted companies will succumb to the pressure. This will only fuel the fire and continue the cycle of this devastating criminal group. "It is more important that the

companies affected are open and honest with their employees and customers offering support in how to protect themselves and how to spot … attacks.”