Hackers behind Microsoft outage most likely Russian-backed group aiming to ‘drive division’ in the west

Publication Date: 2023-06-19

Author: Josh Taylor

Section: Technology

Tags: Cybercrime, Russia, Microsoft, Internet

Article URL: https://www.theguardian.com/technology/2023/jun/19/hackers-behind-microsoft-outage-most-likely-russian-backed-group-aiming-to-drive-division-in-the-west

The hackers believed to be behind a recent attack that took some of Microsoft’s services offline are likely to be a Russian-linked group rather than a grassroots pro-Islam collective operating out of Sudan, experts say. Anonymous Sudan, which surfaced in January 2023, has also claimed responsibility for at least 24 distributed denial-of-service attacks on Australian companies, including healthcare, aviation and education organisations. Last week, Microsoft confirmed that outages to its Outlook service in early June were the result of a DoS attack believed to have been carried out by Anonymous Sudan, which had claimed credit. The group presented itself as a loose group of hacktivists with a name that suggested they were located in Sudan, and it claimed to be targeting Australian organisations in March in protest against clothing worn at Melbourne fashion festival with “God walks with me” written on it in Arabic. Cybersecurity firm CyberCX said in a report released on Monday that the group is unlikely to be an authentic hacktivist organisation and is likely linked to the Russian state, after an analysis of the group’s activities. CyberCX said most hacktivist groups conduct their plans for operations in a semi-public way online, but Anonymous Sudan had only announced targets when they were being attacked, indicating a closely held operation. The firm also said the organisation’s use of paid infrastructure in the attacks – directing mass amounts of traffic to a service in order to bring it down – would have cost tens of thousands of dollars, and was less likely to have been used by a loose collective. CyberCX said Anonymous Sudan was also publicly aligned with pro-Russian threat actors and is a member of the pro-Russia hacker group Killnet. Alastair MacGibbon, CyberCX’s chief strategy officer, told Guardian Australia that Anonymous Sudan’s generally low-level targets and the fact it was presenting itself as an Islamic group indicated a Russian-backed organisation that could be trying to “drive division in society” and disrupt the west. “It really stems from the Russian government proclivities to drive division in society,” he said. “They don’t really care about the issue … anti-racism, pro-environment or whatever – [they] just get into whatever it is that matters to [harm] targets. In this case, the west.” MacGibbon said there appeared to be a growing pattern in the spate of cyber-attacks from Russian-linked hacker groups against Australia. The Optus and Medibank attacks last year were “less monetisable forms of attack”, he said, with the groups threatening to post the data online rather than locking up systems in ransomware attacks. “There has to be a link to other forms of monetisation, potentially a state or some form of direction coming from the state that says ‘go and cause fear, uncertainty and doubt’,” he said. Anonymous Sudan’s Telegram channel has grown to more 60,000 followers since launching.