GCHQ warns of fresh threat from Chinese state-sponsored hackers

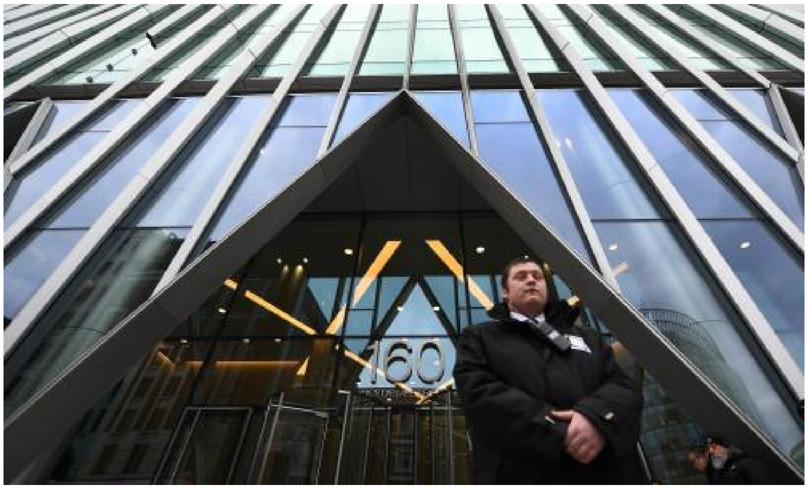
Publication Date: 2023-05-25

Author: Dan Milmo

Section: Technology

Tags: Hacking, Cyberwar, Cybercrime, Espionage, Internet, GCHQ, MI5, news

Article URL: https://www.theguardian.com/technology/2023/may/25/experts-warn-against-china-sponsored-cyber-attacks-on-uk-networks



The UK's cybersecurity agency has urged operators of critical national infrastructure, including energy and telecommunications networks, to prevent Chinese state-sponsored hackers from hiding on their systems. The National Cyber Security Centre, part of GCHQ, issued the warning after it emerged that a Chinese hacking group known as Volt Typhoon had targeted a US military outpost in the Pacific Ocean. The so-called Five Eyes intelligence group – the US, the UK, Australia, Canada and New Zealand – issued a joint notice detailing the nature of the Volt Typhoon threat and how to deal with it. Microsoft said in a separate statement on Thursday that Volt Typhoon had been active since mid-2021 and had targeted telecommunications infrastructure in Guam, an island hosting a US military facility that is expected to play an important role in any American response to an invasion by China of Taiwan. It said organisations had also been targeted in the US, spanning sectors including communications, manufacturing, government, IT and education. Paul Chichester, the NCSC's director of operations, said: "It is vital that operators of critical national infrastructure take action to prevent attackers hiding on their systems, as described in this joint advisory with our international partners. "We strongly encourage providers of UK essential services to follow our guidance to help detect this malicious activity and prevent persistent compromise." One of Volt Typhoon's key tactics was described as "living off the land", or using the existing IT infrastructure of their target to achieve their aims. The joint advisory provided examples of traces left by Volt Typhoon in organisations' systems, so its presence could be detected. The hackers used a "web shell", a piece of malicious code that allows rogue actors to access a web server – and then used that as a way in to connected systems. Secureworks, a US cybersecurity company that contributed to the advisory notice, said Chinese hackers tended to share their techniques with other China-based groups and that similar techniques would be deployed against UK targets. "It is likely that Chinese threat groups will be using similar tradecraft against targets in the UK," said Marc Burnard, a researcher at Secureworks. Don Smith, vice-president of threat research at Secureworks, said the method used by the attackers was akin to "having an evil system administrator on your system". Secureworks said the Chinese attackers targeting US infrastructure had been interested in data "of use to Chinese interests" and were an attempt secure "long term strategic intelligence gain."