MoD contractor hacked by China failed to report breach for months

Publication Date: 2024-05-10

Author: Anna Isaac

Section: Technology

Tags: Hacking, Ministry of Defence, Data and computer security, Cybercrime, Cyberwar, Espionage, Internet, news

Article URL: https://www.theguardian.com/technology/article/2024/may/10/mod-contractor-hacked-china-failed-report-breach-months

The IT company targeted in a Chinese hack that accessed the data of hundreds of thousands of Ministry of Defence staff failed to report the breach for months, the Guardian can reveal. The UK defence secretary, Grant Shapps, told MPs on Tuesday that Shared Services Connected Ltd (SSCL) had been breached by a malign actor and “state involvement” could not be ruled out. Shapps said the payroll records of about 270,000 current and former military personnel, including their home addresses, had been accessed. China has not been openly named by the government as the culprit. The MoD was told of the hack in recent days but a number of sources said SSCL, an arm of the French tech company Sopra Steria, became aware of the breach in February. Sopra Steria did not respond to requests for comment. One Whitehall insider did not comment on the timeframe but said that concern about SSCL being “slow to respond” was one of the issues being examined in an official inquiry into the hack. It can also be revealed that SSCL was awarded a contract worth more than £500,000 in April to monitor the MoD’s own cybersecurity – several weeks after it was hacked. Officials now believe this contract could be revoked. The payroll data that was hacked reflects only a fraction of the work SSCL does for the government. Sopra Steria and SSCL are understood to have other undisclosed government cybersecurity contracts, according to Whitehall sources. However, these are deemed so sensitive that they have never been publicly disclosed. The Cabinet Office declined to comment on the detail of contracts, citing security restrictions. The cybersecurity arm of the UK’s intelligence services, the National Cyber Security Centre, has warned of a growing threat to the country’s businesses and critical national infrastructure from hostile states. Chinese and Russian state-sponsored actors were highlighted among attackers using a range of routes to try to hide malicious activity on networks containing sensitive information. Whitehall worries over a lack of transparency by SSCL have raised concerns that there could be a wider compromise of its systems. Sopra Steria is one of a handful of strategic suppliers to the government, with work ranging from administering pensions to wider payments systems for government departments and agencies. Shapps told parliament that the government had “not only ordered a full review of its [SSCL’s] work within the MoD, but gone further and requested from the Cabinet Office a full review of its work across government, and that is under way”. He added that specialists had been brought in to carry out a “forensic investigation” of how the breach happened. Earlier this week, a spokesperson for the Cabinet Office said: “An independently audited, comprehensive security review of the contractor’s operations is under way and appropriate steps will be taken based on its findings.” SSCL was part-owned by the government until October last year when it sold its 25% stake to Sopra Steria for £82m. SSCL was aware of being a “magnet” for cyber-attacks, sources said. A public warning about identity theft has been on the website of its

parent company, Sopra Steria, for at least three years, according to an examination of the page's history. The hack was first internally detected in February, sources said, with concerns about potentially successful phishing attacks on the company dating back to December 2019. SSCL and its parent company hold a total of £1.6bn in government contracts. These include a range of highly sensitive functions such as Home Office recruitment and online testing for officers, according to information from contracts gathered by the data company Tussell. The Chinese embassy has said China was not responsible for the hack. A spokesperson said: "We urge the relevant parties in the UK to stop spreading false information, stop fabricating so-called China threat narratives, and stop their anti-China political farce."