Cyber-attacks linked to Chinese spy agencies are increasing, say analysts

Publication Date: 2024-03-26

Author: Helen Davidson

Section: Technology

Tags: Cybercrime, Internet, China, Asia Pacific, news

Article URL: https://www.theguardian.com/technology/2024/mar/26/china-cyber-attacks-are-increasing-western-analysts-warn

Cyber-attacks linked to Chinese intelligence agencies are increasing in capability and frequency as they seek to test foreign government responses, analysts have warned in the wake of revelations about a mass hacking of UK data. On Tuesday, the UK and US governments accused hacking group Advanced Persistent Threat 31 (APT 31), backed by China's government spy agency, of conducting a years-long cyber-attack campaign, targeting politicians, national security officials, journalists and businesses. The UK said the hackers had potentially gained access to information on tens of millions of UK voters held by the Electoral Commission, as well as for cyber-espionage targeting lawmakers who have been outspoken about threats from China. Both the US and UK governments announced sanctions against linked Chinese companies and individuals. Also on Tuesday, the New Zealand government said it had raised concerns with the Chinese government about its involvement in an attack which targeted the country's parliamentary entities in 2021. Analysts told the Guardian there were clear signs of an increase in cyber-attacks which appeared to be conducted by Chinese actors, often with links to China's intelligence agencies and government. "Some of the hacking groups are information security firms contracted to Chinese intelligence units to carry out attacks on specific targets, such as the recent case of iSoon Information," said analyst Che Chang, from Taiwan-based cyber threat analysis firm TeamT5. TeamT5 had monitored an increase in "constantly evolving" hacking efforts by Chinese groups in the Pacific region and Taiwan over the last three years. "We believe that their purpose is to infiltrate specific targets and steal important information and intelligence, whether it be political, military or commercial," Chang said. Chang said there was not sufficient information to specifically trace the activity all the way to China's top leadership (and Beijing resolutely rejects the allegations), but "given China's system of no distinction between party and state, it is true that we cannot rule out the possibility of instructions coming from the top". Several analysts said western governments, however, have become much more willing to name China as the perpetrator, after years of avoiding antagonising the leaders of the world's second largest economy. "That earlier reticence to criticise has given way to a more vocal stance and I think that's probably because the scale of the threat and the actual intrusions has risen. They are more serious threats now," said David Tuffley, a senior lecturer in cybersecurity at Griffith University in Australia. The UK announcement followed revelations last month that a Chinese hacking network known as Volt Typhoon had been lying dormant inside US critical infrastructure for as long as five years, "pre-positioning" itself for future acts of sabotage. That operation sparked alarm among Five Eyes observers as it indicated a shift away from intelligence-gathering espionage towards warfare preparation. Tuffley said cyber-attacks were part of China's greyzone activity – meaning acts that approach but do not

reach the threshold of warfare. Much of the activity is regionally focused, targeting Taiwan and other countries disputing claims in the South China Sea. But these cyberattacks had a far broader reach. “The whole point to make about all of this is that China is obviously adopting a much more muscular stance,” said Tuffley. “It knows it doesn’t have the military capability to defeat the Americans, the British, Australians, Japanese and Koreans, in a hot war. So they are most unlikely to take it to that point.” Instead it is seeking to cause instability in the target country, and “perhaps a loss of confidence in the operational abilities of that target”. It is also testing its own capabilities up against adversaries’ defences, he said. Tuffley said there was a danger of escalation. Other governments like the US and UK had high cyber-espionage capabilities themselves, but were not publicly threatening countermeasures against the Chinese state. In its statement on Tuesday US authorities named individuals accused of conducting the cyber attacks allegedly in breach of US law. That suggested a deep level of knowledge about the attacks, including perhaps through human intelligence sources inside the Chinese operations, or a retaliatory information-gathering hack, one analyst said. “Anyone who has worked in cybersecurity for any amount of time will not be at all surprised by this report from the UK authorities,” said Adam Marrè, chief information security officer at Arctic Wolf. “Beijing continues to see cyber as a natural extension of their statecraft and have seldom been afraid to utilise cyber techniques to further their own national interests.” This article was amended on 27 March 2024 to correct the spelling of Che Chang’s name