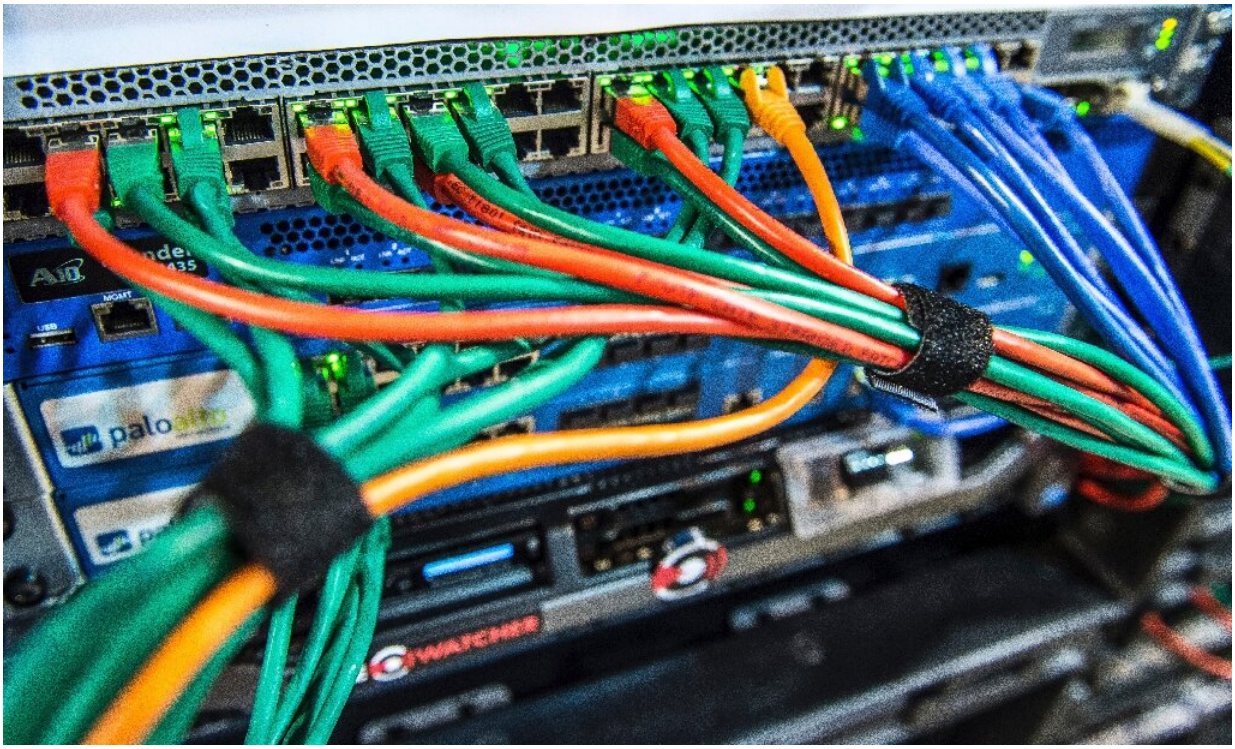
Australia under cyberattacks from state actor

June 19 2020, by Andrew Beatty



Australia warns the country is under a broad cyberattack from a 'state-based actor' targeting government, public services and businesses

Australia's prime minister revealed Friday his country was under a broad cyberattack from a "state-based actor" targeting government, public services and businesses, with suspicions falling on China.

Warning Australians of "specific risks" and an increased tempo of

attacks, Scott Morrison told a press conference that a range of sensitive institutions had been hit.

"This activity is targeting Australian organisations across a range of sectors, including all levels of government, industry, political organisations, education, health, essential service providers and operators of other critical infrastructure," he said.

Morrison levelled blame at a "sophisticated state-based cyber actor", but declined to name the culprit, while saying that it could only come from one of a handful of states.

China, Iran, Israel, North Korea, Russia, the United States and a number of European countries are known to have developed advanced cyberwarfare capabilities.

But suspicions immediately fell on Beijing, which has clashed repeatedly with Canberra as it looks to increase the cost of Australia speaking out against Communist Party interests.

Most recently Australia enraged China by calling for an investigation into the origins of the coronavirus pandemic.

But Canberra has also pushed back against what it describes as China's economic "coercion", covert influence campaigns and the use of technology companies like Huawei as a tool of intelligence gathering and geopolitical leverage.

China has warned its students and tourists against going to Australia, slapped trade sanctions on Australian goods and sentenced an Australian citizen to death for drug trafficking.

Last year Australia's parliament, political parties and universities were

targeted by state-backed cyberattacks, with China seen as the likely culprit.

Public broadcaster ABC cited "senior sources" confirming that China was believed to be behind today's ongoing attacks as well.

Chinese foreign ministry spokesman Zhao Lijian said Friday that China was "a staunch defender of cybersecurity" and has "always resolutely opposed and cracked down on all forms of cyberattacks".

Beijing has previously described such allegations as "irresponsible" and an attempt to "smear" China.

Experts say attribution is often difficult, time-consuming and, if made public, could escalate tensions further.

Beijing and Canberra have also sparred over access to natural resources, maritime claims and the use of Chinese state-backed technology companies

'Malicious'

The current attack appears designed to hide authorship, using so-called "copy-paste" cyber tools that can be easily found open source, Australia's signals intelligence agency said.

They included "proof-of-concept exploit code" that targeted vulnerabilities in old versions of Microsoft, Telerik, SharePoint and Citrix products as well as "web shell" software that is uploaded and remains on compromised servers.

The attacks also used "spearfishing" techniques, sending emails with malicious files, links and Office 365 prompts.

Morrison said that he had notified the leader of the opposition and state premiers of the "malicious" cyberattacks, but said no personal data had been compromised and many of the attacks were unsuccessful.

"They are not new risks, but they are specific risks," he said.

"We encourage organisations, particularly those in the health, critical infrastructure and essential services to take expert advice and to implement technical defences," he said.

That warning is likely to raise alarm bells as the country's medical facilities—already on crisis footing because of the coronavirus

pandemic—could come under further strain.

Morrison's vagueness about the threat and its source is deliberate, according to Ben Scott, a former Australian intelligence official now with the Lowy Institute, a think tank.

"Public attribution – and the threat of doing so -– is seen as one way of warning and deterring an opponent," he said.

"But early attribution can also be provocative," he added, saying China was "almost certainly" behind the attack.

"Australian agencies may hope that the PM's statement will deter the attackers from moving on to extract large volumes of information or engaging in any sabotage."

Australia is part of the Five Eyes intelligence-sharing network—along with Britain, Canada, New Zealand and the United States—which give the country access to advanced capabilities, but also makes it a rich target for adversaries.