CHINA GUILTY

RECENT GLOBAL CYBER ATTACKS

UNITED KINGDOM: Chinese hackers accessed the details of more million patients in May, including 2000 credit card numbers.

UNITED STATES: The FBI warned that Chinese hackers were attempting to steal valuable intellectual property and critical health data related to a coronavirus vaccine in May.

GERMANY: A Russian hacking group reportedly hacked into energy and power companies in May.

AUSTRIA: Companies including Fisher & Paykel Appliances, Avanz and Unilever have suffered cyber attacks and data breaches.

WHAT COUNTRY IS BEHIND THE ATTACKS?

The government has not named the state actor but has suggested it involved third-party security firms and a Chinese whom was behind the attack.

IS AUSTRALIA BEING TARGETED?

Yes. The attacker is selecting targets carefully.

WHAT IS FIVE EYES?

The Five Eyes is an intelligence sharing alliance comprising Australia, Canada, New Zealand, the UK and the US. It has major private communications worldwide.

A stylized map of the world with a spotlight on China is shown.

MICHAEL WARD

ELLEN WHINNAET

CYBER space targeting Australia's most sensitive secrets has attacked all levels of government and critical infrastructure, with China accused of orchestrating the sneak attack and successfully infiltrating some networks.

The Prime Minister Scott Morrison yesterday slammed the "sophisticated state-based attack" for an attack targeting Australian businesses, political organisations, education and health providers and all levels of government.

He refused to name the foreign government or agency, but his senior government and security sources told The Courier-Mail China was behind the extraordinary move.

But the Chinese Government last night rejected claims it was to blame for the cyber attack, with a spokesman saying the "attackers are completely baseless".

Security experts described the cyber hit as an "advanced persistent threat" orAPT that would use sophisticated methods to hide the attacker's tracks.

WHAT IS THE DAMAGE?

The cyber attack targeting Australia's critical systems is said to be "devastating".

PM Scott Morrison said the "damage" to the Australian economy would be "significant".

WHAT IS THE RISK?

The risk of a cyber attack targeting Australia's critical systems is said to be "very high".

WHAT IS THE SOLUTION?

Australia's intelligence agencies are working around the clock to mitigate the risk of a cyber attack targeting its critical systems.

Cyber Security Chair Ryan Ko said attacks persistently scored for vulnerabilities in any device connected to the internet before moving to gain "deep access".

A 48-page report released by the Australian Cyber Security Centre labeled the attacks "deeply concerning" because they were "very sophisticated".

Prime Minister Scott Morrison has refused to name China as the "state actor" behind the cyber attack on Australia and Indonesia.

China's President Xi Jinping is shown on the cover image with the headline "ALL BUT THE NAME".
Profile cyber attacks including one that disrupted operations at Brisbane's XXXX brewery.

The Government's intervention was widely interpreted as a warning to let China know their spying had been detected as well as an urgent call to arms for businesses to update their systems to avoid cyber intrusions.

Mr Morrison said the attacks were ongoing.

Australian Strategic Policy Institute executive director Peter Jennings said the finger was "squarely pointed at China" with the "very high certainty" they were responsible.

Tom Uren from the Australia Strategic Policy Institute's international cyber policy centre said Mr Morrison was "talking about the Chinese state and some groups conducting espionage on their behalf."

He said while Russia, Iran and North Korea had sophisticated capabilities, "none of these countries had the same motivation" as China to attack Australia.

A 48-page report released by the Australian Cyber Security Centre labelled the attacks "copy-paste compromises" because the attackers copied publicly available code from public domains and the dark web to exploit networks.

University of Queensland Cyber Security Chair Ryan Ko said attackers persistently searched for vulnerabilities in any device connected to the internet before moving to targeted "spear phishing" if they could not find a way in.

The ACSC report revealed the spear phishing operations included using links to credential harvesting websites, sending emails with links to malicious files or with the malicious files directly attached and email tracking services.

Prof Ko said targets were tricked into typing a password that could be stolen or opening an email that downloaded software on the computer that "calls back to the mother ship of the attacker."

He said the most worrying aspect was that once attackers infiltrated a "high value target" they could use a compromised machine as a "base". The government said no "large-scale personal data breaches" were detected.