China blamed for 'massive' cyber attack on Bureau of Meteorology computer

By political editor Chris Uhlmann

Updated Wed 2 Dec 2015, 8:28pm

China is being blamed for a major cyber attack on the computers at the Bureau of Meteorology, which has compromised sensitive systems across the Federal Government.

Multiple official sources have confirmed the recent attack, and the ABC has been told it will cost millions of dollars to plug the security breach, as other agencies have also been affected.

The bureau owns one of Australia's largest supercomputers and provides critical information to a host of agencies.

Its systems straddle the nation, including one link into the Department of Defence at Russell Offices in Canberra.

Cyber attacks on government agencies are routine and the "adversaries" range from thrill-seeking hackers, through to criminals and foreign states.

But the ABC has been told this is a "massive" breach and one official said there was little doubt where it came from.

"It's China," he said.

But, China has denied any involvement in the attack.

"As we have reiterated on many occasions, the Chinese government is opposed to all forms of cyber attacks," Chinese foreign ministry spokeswoman Hua Chunying said.

"We have stressed that cyber security needs to be based on mutual respect.

"We believe it is not constructive to make groundless accusations or speculation."

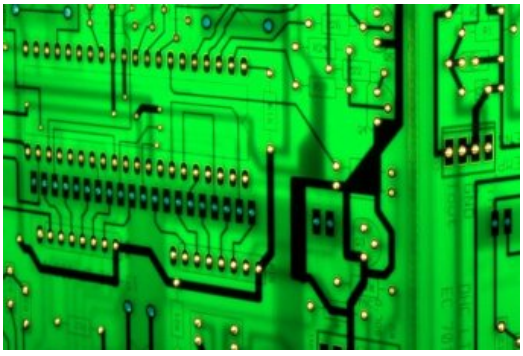

PHOTO: The attack on the BoM computer system has been described as 'massive' (Flickr: Nick Miller)

RELATED STORY: Chinese military unit accused of hacking attacks

RELATED STORY: Why we should all care about cyber crime: the risk to you and me

MAP: Australia

Key points:

- ABC told there is little doubt the "massive" breach came from China
- Motivation for attack could be commercial, strategic or both
- Bureau provides critical information to a host of agencies, including link to Defence Department
- Could "take years and cost hundreds of millions of dollars to fix"

Australian Strategic Policy Institute (ASPI) executive director Peter Jennings said there was evidence China was behind the hack.

"We certainly know that among the most active intelligence gatherers is Chinese intelligence," Mr Jennings said.

"So what we understand of the Chinese attack on the BoM is entirely consistent with what we know of how Chinese intelligence operates."

The motivation for the attack on the bureau could be commercial, strategic or both.

The bureau is a critical national resource and another state would place a high value on its intellectual property and scientific research.

In the event of a conflict, compromising Australia's ability to accurately forecast weather would affect the operation of military and commercial aircraft.

Beyond that, the bureau provides a gateway to other agencies.

"They're looking for the weakest link and so if you go into an agency, which may have a level of security clearance, but perhaps not as high as central parts of the national security community, maybe there are weaknesses they can exploit which will enable them to then move into other, more highly-valued targets," Mr Jennings said.

'Range of adversaries' motivated to target networks

A spokesman for Prime Minister Malcolm Turnbull said a range of adversaries, including "state-sponsored actors and serious organised criminals", were motivated to attack government networks.

"The Government's aware of a press report that the Bureau has been the subject of a cyber attack," the spokesperson said in a statement, adding the Government would not comment on specific cases.

"The Government takes any cyber attacks seriously and is currently reviewing its cyber security policy."

The bureau did not deny the attack, and said its systems were working.

"Like all government agencies, we work closely with the Australian Government security agencies," it said in a statement.

"The bureau's systems are fully operational and the bureau continues to provide reliable, ongoing access to high quality weather, climate, water and oceans information to its stakeholders."

In March the Bureau's chief executive Dr Robert Vertessy told Radio National that his agency had evolved "from what was once just a straight weather service to what I would call now a more broad-based environmental intelligence agency".

It provides weather and climate forecasting, tsunami warnings, tide predictions, water resources and even space weather.

There is no clear picture yet how much the breach will cost to fix or how long it will take but the critical nature of the bureau's services means its systems cannot be switched off for repair.

In the words of one source: "It could take years and cost hundreds of millions of dollars to fix."

Cyber attacks traced to Chinese army building in Shanghai

PHOTO: Locals walk in front of Unit 61398, a secretive Chinese military unit, on the outskirts of Shanghai (Reuters: Carlos Barria)

The United States has repeatedly blamed China for cyber attacks on its agencies and American businesses. At a meeting in September, US president Barack Obama raised it with his Chinese counterpart Xi Jinping.

The Chinese president warned against politicising the issue and said China had a lot to lose from cyber crime.

China has noted that America also devotes a lot of resources to cyber warfare, as do many other countries.

Australia has been recruiting cyber warriors, with the Australian Signals Directorate hiring IT professionals who can put themselves "in the shoes of the hacker".

The most detailed publicly available study of China's capabilities was published by American computer security firm Mandiant in 2013.

Mandiant tracked dozens of groups around the world but focused on one of the most prolific, which it traced to a People's Liberation Army building in Shanghai, Unit 61398.

The report said the reason the unit was "able to wage such a long-running and extensive cyber espionage campaign in large part because it receives direct government support".

In its first unclassified threat report this year the Australian Cyber Security Centre said the cyber threat to Australia is "undeniable, unrelenting and continues to grow".

The Centre said it "sees daily cyber espionage activity targeting Australian Government networks".

"Cyber adversaries will target the weakest link; if the network security of their primary target is robust, they will move to secondary targeting of other networks that may hold the same information but are easier to compromise.

"A cyber adversary is an individual or organisation (including an agency of a nation state) that conducts cyber espionage, crime or attack.

"Foreign state-sponsored adversaries, including nation-states, seek economic, foreign policy, defence and security information for strategic advantage. Such adversaries have traditionally possessed the most advanced and sophisticated tools to conduct their activities, sometimes maintaining access to an organisation's network for years at a time to steal the information they require. These adversaries are most frequently identified as Advanced Persistent Threats (APT)."

Topics: government-and-politics, security-intelligence, defence-and-national-security, federal-government, australia, china, asia

First posted Wed 2 Dec 2015, 11:19am