Source : www.idsa.in Date : 2020-07-15

DECODING CYBERATTACK ON AUSTRALIA

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

More from the author

The sudden outbreak of COVID-19 has led to increased use of digital platforms as primary modes of communication as well as transaction. However, lack of adequate cybersecurity measures has opened up multiple entry points for malicious cyber actors to exploit the network and system vulnerabilities to their advantage.

Recently, several public and private-sector organisations in Australia encountered massive cyberattacks. On June 19, Prime Minister Scott Morrison stated that these attacks are “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.” Referring to the scale and nature of the targeting and the tradecraft used, he described the attacker as “a sophisticated state-based cyber actor”.1 Australian Defence Minister Linda Reynolds too stated that malicious cyber-activity is “increasing in frequency, scale, in sophistication and in its impact”.2

Though Prime Minister Morrison avoided making any public attribution to the *state-based cyber actor*, a few days later, the Australian authorities raided the house and office of a New South Wales lawmaker for his alleged links with the Chinese Government.3 In fact, for the past few months, Australia has been a constant target of large scale cyberattacks by a foreign country.4

Last year, in February 2019, the hackers had breached the computer network of the Australian Parliament. The Australian Signals Directorate (ASD) investigation subsequently revealed that perpetrators had also entered the networks of the ruling Liberal Party, its coalition partner the Nationals, and the opposition Labour Party.5 The attack came at a time when the country was preparing for elections. This incident was similar to the cyberattack on the Democratic Party institutions in the United States (US) ahead of the 2016 election. However, there was no concrete indication that the information gathered by the hackers was used in any way to influence the election results.

In view of the sustained targeting of government organisations and private companies, the Australian Cyber Security Centre remains on high alert. The attackers have used common “copy-paste compromises” which was deciphered on investigations from the cyber actor’s heavy use of “proof-of-concept” exploit code, web shells and other tools copied from open source.6

Attackers are primarily using “remote code execution vulnerability” to target the country’s network and systems. It is a common form of cyberattack in which the perpetrator tries to insert its own software code into vulnerable systems such as a server or database.7 This attempt could have been carried out by customised “spear-phishing” techniques, like sending targets links to malicious files and websites aimed at harvesting passwords.8 However, according to Prime Minister Morrison, though such activity is not new but its frequency has been increasing over many months. He added that the investigations conducted so far have not revealed any large-scale personal data breaches of Australians’ private information.9

The Australian Strategic Policy Institute found that the attack was “95 percent or more” likely to have been launched from China because of its scale and intensity.10 Additionally, Australian investigators found that the attacker used codes and techniques known to have been used by China in the past. Prime Minister Morrison’s comment that “there are not a large number of

state-based actors that can engage in this type of activity" has also been interpreted as a coded reference to China.[11] These attacks came at a time when the two countries were falling out over the origins of the coronavirus wherein Australia attempted to launch a UN investigation into China's role in the origins of the virus.[12] The tension between the two countries has been growing over a host of issues including trade, travel and, most recently, the death sentence handed over to an Australian citizen Karm Gilespie, allegedly a drug smuggler.[13]

China has denied any role in the cyberattacks, saying such accusations are "totally baseless". China feels that they have been the biggest victims of cyber espionage and cyber attacks and Australia being part of the Five Eyes intelligence alliance has consistently been obsessed with such actions.[14]

China has also put economic sanctions on some Australian imports and threatened to boycott Australian goods.[15] It is Australia's largest trading partner, buying more than one-third of the country's total exports. Over a million Chinese tourists and students travel to Australia annually. Australian authorities had earlier reportedly acknowledged that there is a "very real prospect of damaging the economy" if it publicly accuses China over the attack.[16]

In April 2020, the World Health Organisation (WHO) had noted a sudden spike in the number of cyberattacks during the pandemic.[17] There were instances of attempted breaches to draw out details of ongoing research on the COVID-19 vaccine.[18] Even Canada announced that its intellectual property linked to the pandemic research is a "valuable target" of foreign espionage and interference.[19] Often these attacks have been linked to China. However, except for the US, most of the countries have been reluctant to point to the sources of cyberattacks.

A cybersecurity firm, Cyfirma, has also warned India against a potential large-scale cyberattack in view of ongoing tensions with China.[20] On June 19, the Indian Computer Emergency Response Team (CERT-In) issued an advisory about a planned large-scale phishing attack campaign against India.[21] Cyfirma had gathered the information based on conversations taking place in the Chinese hacker forum on the dark web. The firm traced the list back to their sources and found links to two hacking groups, Gothic Panda and Stone Panda. These groups are known to have a direct affiliation to the People's Liberation Army (PLA).[22] Subsequently, on June 23, Maharashtra Cyber, the state police cyber wing, stated that "at least 40,300 cyber attacks were attempted in the last four-five days on the resources in Indian cyberspace".[23] Meanwhile, India has banned 59 apps reportedly linked to the Chinese Government and involved in data extraction for coercive purposes.[24]

The Australian Government has announced that it is recruiting 500 additional cyberspies and would allocate US$ 98 million to strengthen the country's cybersecurity amidst escalating tensions due to suspicion of meddling and espionage by foreign countries.[25] However, the central question remains: Is this enough?

While fortifying cybersecurity is an important step, one cannot build a dam when the storm is overhead. Cybersecurity should be seen as an action akin to patrolling borders wherein constant vigilance is required.

It is equally important to curate a response such that it deters future actions of perpetrators. However, state actors often hide behind the so-called independent non-state actors, making attribution of cyberattacks a tough task. In such cases, based on effective cyber forensics, pattern research and trace-back mechanism, states should come together to build a proportionate response for deterring malicious actions.

Until then, with the adoption of varied digital means to continue business as usual in times of

pandemic, the states are likely to witness increased cyberattacks. Absence of an effective response would only mean an open playground for perpetrators.

Views expressed are of the author and do not necessarily reflect the views of the IDSA or of the Government of India.

END

Downloaded from **crackIAS.com**

© **Zuccess App** by crackIAS.com

crackIAS.com