Source : www.thehindu.com Date : 2022-02-25

U.S. GROUP HACKED INDIAN RESEARCH INSTITUTES: CHINA FIRM

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

A new report from a Beijing-based cybersecurity firm said hackers linked with the U.S. National Security Agency (NSA) were found to have inserted “covert backdoors” that may have given them access to sensitive information in dozens of countries, including India, Russia, China and Japan.

Among the reportedly compromised websites listed in the report were those linked to one of India’s top microbial research labs — the Institute of Microbial Technology (IMTech) under the Council of Scientific and Industrial Research — as well as the Indian Academy of Sciences in Bengaluru. Websites linked to Banaras Hindu University were also listed as being hacked into.

‘Backdoors found’

The Beijing-based cybersecurity firm Pangu Lab released a technical report explaining how it had found the backdoors and linked it to “unique identifiers in the operating manuals of the NSA” that had come to light in the 2013 leak of NSA files by insiders. “In 2016 and 2017,” the report said, “the ‘Shadow Brokers’ published two batches of hacking files claimed to be used by ‘The Equation Group’.

In these hacking files, researchers from Pangu Lab found the private key that can be used to remotely trigger the backdoor Bvp47…a hacker tool belonging to ‘The Equation Group’.

Through further research, the researchers found that the multiple procedures and attack operation manuals disclosed by the ‘Shadow Brokers’ are completely consistent with the only identifier used in the NSA network attack platform operation manual exposed by CIA analyst Snowden in the PRISM incident in 2013.”

The report, which explained the technicalities of how the backdoor worked, said this was “a backdoor communication technology that has never been seen before, implying an organisation with strong technical capabilities behind it”.

“As an advanced attack tool, Bvp47 has allowed the world to see its complexity,” it said. “What is shocking is that after analysis, it has been realised that it may have existed for more than 10 years.”

The report listed dozens of sites — many universities and scientific research institutes — that had reportedly been compromised in countries, including both U.S. adversaries and allies and partners, ranging from India and Japan to China and Russia.

The report is being framed by the Chinese media as a rebuttal to U.S. allegations of Chinese cyberhacking.

China-linked cyberattacks have targeted a number of U.S. institutions and become a thorny issue in U.S.-China relations.

Indian agencies have reported cyber attacks from China targeting a wide range of institutions, including government departments.

The Union Power Ministry said last year that “state-sponsored” Chinese hacker groups had targeted various Indian power centres but added that the groups have been thwarted after government cyber agencies warned about their activities.

This followed a report from a U.S. cybersecurity firm linking a major power outage in Mumbai in 2020 to hacking attacks by China-linked groups.

Our code of editorial values

END

Downloaded from **crackIAS.com**

© **Zuccess App** by crackIAS.com