China calls hacking report 'far-fetched' and accuses the US of targeting the cybersecurity industry

June 16 2023

Chinese Foreign Ministry spokesperson Wang Wenbin speaks during a press conference at the Ministry of Foreign Affairs in Beijing, Friday, June 16, 2023. China's government on Friday rejected as "far-fetched and unprofessional" a report by a U.S. security firm that blamed Chinese-linked hackers for attacks on hundreds of public agencies, schools and other targets around the world. Credit: AP Photo/Liu Zheng

China's government on Friday rejected as "far-fetched and unprofessional" a report by a U.S. security firm that blamed Chinese-linked hackers for attacks on hundreds of public agencies, schools and other targets around the world.

A foreign ministry spokesperson repeated accusations that Washington carries out hacking attacks and complained the cybersecurity industry rarely reports on them.

Mandiant's report came ahead of a visit to Beijing by Secretary of State Antony Blinken aimed at repairing relations that have been strained by disputes over human rights, security and other irritants. Blinken's visit was planned earlier this year but was canceled after what the U.S. government said was a Chinese spy balloon flew over the United States.

The report said hackers targeted email to engage in "espionage activity in support of the People's Republic of China."

"The relevant content is far-fetched and unprofessional," said the Chinese spokesperson, Wang Wenbin.

"American cybersecurity companies continue to churn out reports on so-called cyberattacks by other countries, which have been reduced to accomplices for the U.S. government's political smear against other countries," Wang said.

The latest attacks exploited a vulnerability in a Barracuda Networks email system and targeted foreign ministries in Southeast Asia, other government agencies, trade offices and academic organizations in Taiwan and Hong Kong, according to Mandiant.

The American and Chinese flags wave at Genting Snow Park ahead of the 2022 Winter Olympics, in Zhangjiakou, China, on Feb. 2, 2022. Hackers linked to China were likely behind the exploitation of a software security hole in cybersecurity firm Barracuda Networks' email security feature that affected public and private organizations globally, according to an investigation by security firm Mandiant. Credit: AP Photo/Kiichiro Sato, File

It described the attacks as the biggest cyber espionage campaign known to be conducted by a "China-nexus threat actor" since a 2021 attack on Microsoft Exchange. That affected tens of thousands of computers.

China is regarded, along with the United States and Russia, as a leader in the development of computer hacking for military use. Security

consultants say its military also supports hobbyist hacking clubs that might work for outsiders.

Barracuda announced on June 6 that some of its its email security appliances had been hacked as early as October, giving the intruders a back door to compromised networks.

Mandiant said the email attacks focused on issues that are priorities for China, particularly in the Asia Pacific region. It said the hackers searched for email accounts of people working for governments of political or strategic interest to China at the time they were participating in diplomatic meetings.

Earlier this year, Microsoft said state-backed Chinese hackers have been targeting U.S. critical infrastructure and could be laying the technical groundwork for the potential disruption of critical communications between the U.S. and Asia during future crises.