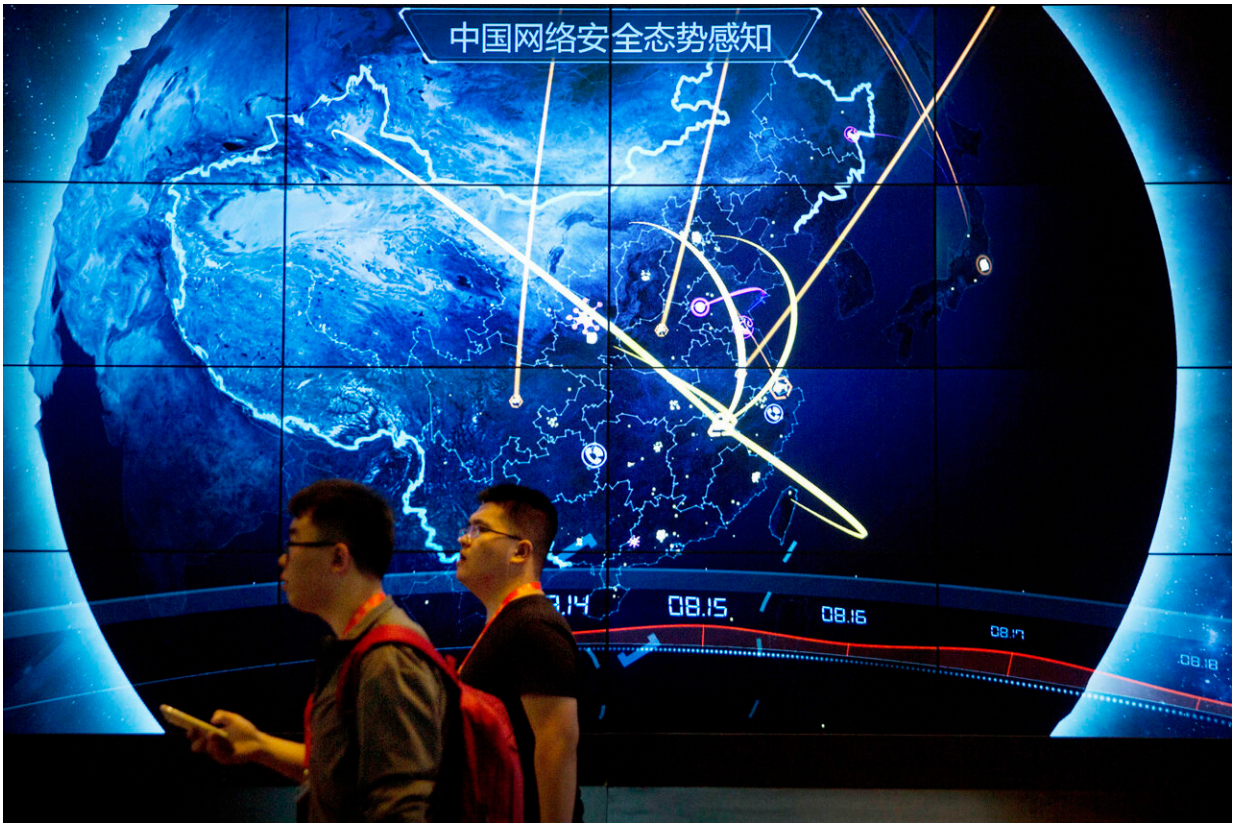
Chinese spies breached hundreds of public, private networks, security firm says

June 15 2023, by Frank Bajak



Attendees walk past an electronic display showing recent cyberattacks in China at the China Internet Security Conference in Beijing, on Sept. 12, 2017. 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/Mark Schiefelbein, File

Suspected state-backed Chinese hackers used a security hole in a popular email security appliance to break into the networks of hundreds of public and private sector organizations globally, nearly a third of them government agencies including foreign ministries, the cybersecurity firm Mandiant said Thursday.

"This is the broadest cyber espionage campaign known to be conducted by a China-nexus threat actor since the mass exploitation of Microsoft Exchange in early 2021," Charles Carmakal, Mandiant's chief technical officer, said in a emailed statement. That hack compromised tens of thousands of computers globally.

In a blog post Thursday, Google-owned Mandiant expressed "high confidence" that the group exploiting a software vulnerability in Barracuda Networks' Email Security Gateway was engaged in "espionage activity in support of the People's Republic of China." It said the activivity began as early as October.

The hackers sent emails containing malicious file attachments to gain access to targeted organizations' devices and data, Mandiant said. Of those organizations, 55% were from the Americas, 22% from Asia Pacific and 24% from Europe, the Middle East and Africa and they included foreign ministries in Southeast Asia, foreign trade offices and academic organizations in Taiwan and Hong Kong. the company said.

Mandiant said the majority impact in the Americas may partially reflect the geography of Barracuda's customer base.

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 into compromised networks. The hack was so severe the California company recommended fully replacing the appliances.

After discovering it in mid-May, Barracuda released containment and remediation patches but the hacking group, which Mandiant identifies as UNC4841, altered their malware to try to maintain access, Mandiant said. The group then "countered with high frequency operations targeting a number of victims located in at least 16 different countries."

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

Word of the breach arrived with U.S. Secretary of State Antony Blinken departing for China this weekend as part of the Biden administration's push to repair deteriorating ties between Washington and Beijing.

His visit had initially been planned for early this year but was postponed indefinitely after the discovery and shootdown of what the U.S. said was a Chinese spy balloon over the United States.

Mandiant said the targeting at both the organizational and individual account levels, focused on issues that are high policy 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 with other countries.

In a emailed statement Thursday, Barracuda said about 5% of its active Email Security Gateway appliances worldwide showed evidence of potential compromise. It said it was providing replacement appliances to affected customers at no cost.

The U.S. government has accused Beijing of being its principal cyberespionage threat, with state-backed Chinese hackers stealing data from both the private and public sector.

In terms of raw intelligence affecting the U.S., China's largest electronic infiltrations have targeted OPM, Anthem, Equifax and Marriott.

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.

China says the U.S. also engages in cyberespionage against it, hacking

into computers of its universities and companies.