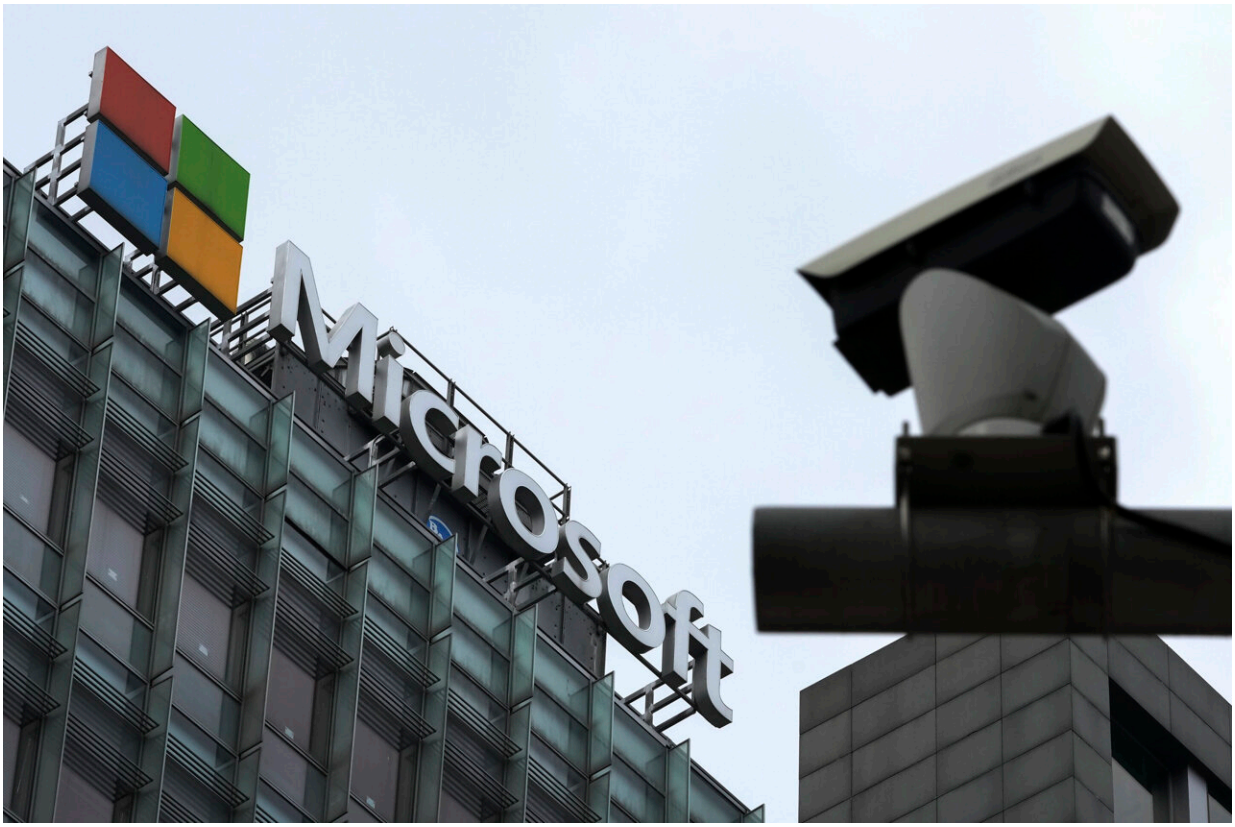
Microsoft: State-sponsored Chinese hackers could be laying groundwork for disruption

May 25 2023, by Frank Bajak



A security surveillance camera is seen near the Microsoft office building in Beijing, July 20, 2021. 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, Microsoft said Wednesday, May 24, 2023. Credit: AP Photo/Andy Wong, File

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, Microsoft said Wednesday.

The targets include sites in Guam, where the U.S. has a major military presence, the company said.

Hostile activity in cyberspace—from espionage to the advanced positioning of malware for potential future attacks—has become a hallmark of modern geopolitical rivalry.

Microsoft said in a blog post that the state-sponsored group of hackers, which it calls Volt Typhoon, has been active since mid-2021. It said organizations affected by the hacking—which seeks persistent access—are in the communications, manufacturing, utility, transportation, construction, maritime, information technology and education sectors.

Separately, the National Security Agency, the FBI, the Cybersecurity and Infrastructure Security Agency (CISA) and their counterparts from Australia, New Zealand, Canada and Britain published a joint advisory sharing technical details on "the recently discovered cluster of activity."

A Microsoft spokesman would not say why the software giant was making the announcement now or whether it had recently seen an uptick in targeting of critical infrastructure in Guam or at adjacent U.S. military facilities there, which include a major air base.

John Hultquist, chief analyst at Google's Mandiant cybersecurity intelligence operation, called Microsoft's announcement "potentially a really important finding."

"We don't see a lot of this sort of probing from China. It's rare," Hultquist said. "We know a lot about Russian and North Korean and Iranian cyber-capabilities because they have regularly done this." China has generally withheld use of the kinds of tools that could be used to seed, not just intelligence-gathering capabilities, but also malware for disruptive attacks in an armed conflict, he added.

Microsoft said the intrusion campaign placed a "strong emphasis on stealth" and sought to blend into normal network activity by hacking small-office network equipment, including routers. It said the intruders gained initial access through internet-facing Fortiguard devices, which are engineered to use machine-learning to detect malware.

The maker of Fortiguard devuces, Fortinet, did not immediately respond to an email seeking further details.

"For years, China has conducted aggressive cyber operations to steal intellectual property and sensitive data from organizations around the globe," said CISA Director Jen Easterly, urging mitigation of affected networks to prevent possible disruption. Bryan Vorndran, the FBI cyber division assistant director, called the intrusions "unacceptable tactics" in the same statement.

Tensions between Washington and Beijing—which the U.S. national security establishment considers its main military, economic and strategic rival—have been on the rise in recent months.

Those tensions spiked last year after then-House Speaker Nancy Pelosi's visit to democratically governed Taiwan, leading China, which claims the island as its territory, to launch military exercises around Taiwan.

U.S.-China relations became further strained earlier this year after the U.S. shot down a Chinese spy balloon that had crossed the United States.