China Admitted to Volt Typhoon Cyberattacks on US Critical Infrastructure: Report

By Eduard Kovacs

Published: 2025-04-11 · Archived: 2026-04-05 20:02:36 UTC

In a secret meeting that took place late last year between Chinese and American officials, the former confirmed that China had conducted cyberattacks against US infrastructure as part of the campaign known as Volt Typhoon, according to The Wall Street Journal.

The meeting took place at a Geneva summit in December and involved members of the outgoing Biden administration. The US officials who were present were startled by China's admission, people familiar with the matter told WSJ [paywalled article].

The remarks made at the meeting by Chinese officials were "indirect and somewhat ambiguous", but the American delegation interpreted that the attacks tracked as Volt Typhoon were conducted in response to the US supporting Taiwan, WSJ reported.

The conclusion of American officials after the meeting was that the cyberattacks were meant to scare the United States from getting involved in a potential conflict between China and Taiwan.

The Volt Typhoon attacks, which were attributed to China immediately after their discovery, involved the use of zero-day vulnerabilities and other sophisticated techniques. The attacks were aimed at critical infrastructure and raised concerns that they could enable China to spy on the US and cause significant disruptions.

The Volt Typhoon threat actors managed to gain access to systems in a wide range of sectors, including communications, manufacturing, utility, construction, government, IT, maritime, transportation, and energy. It came to light recently that the hackers managed to dwell in the US electric grid for 300 days in 2023.

According to WSJ, the Salt Typhoon attacks aimed at several major American telecom firms, which had come to light in the months leading up to the December meeting in Geneva, were also mentioned during the meeting, but the focus was on the Volt Typhoon attacks.

The Salt Typhoon campaign resulted in the phone calls and text messages of senior officials getting compromised. Unlike the Volt Typhoon attacks, which the US sees as an unacceptable provocation, the Salt Typhoon campaign is similar to cyberespionage that the US itself conducts against its adversaries.

In recent years both the US and China have stepped up their game in publicly accusing each other of conducting cyberattacks.

Related: Hackers Could Unleash Chaos Through Backdoor in China-Made Robot Dogs

Related: Despite Rip-and-Replace Efforts, FCC Suspects Banned Chinese Telecom Providers Still Active in US

Related: Chinese I-Soon Hackers Hit 7 Organizations in Operation FishMedley

---