

Chinese hackers infiltrated plane, train and water systems for five years, US says

Publication Date: 2024-02-08

Author: Unknown

Section: Technology

Tags: Technology, Hacking, China, Cyberwar, Canada, New Zealand, news

Article URL: <https://www.theguardian.com/technology/2024/feb/08/chinese-hack-us-transportation-infrastructure>



An advanced group of Chinese hackers taking aim at critical US infrastructure has been active for as long as half a decade, American and allied intelligence agencies said in a joint statement on Wednesday. The US National Security Agency, US cyber watchdog CISA, the FBI and the Transportation Security Administration said that the group known as Volt Typhoon had quietly burrowed into the networks of aviation, rail, mass transit, highway, maritime, pipeline, water and sewage organizations. None of the organizations were identified by name, but the statement said that US intelligence officials had observed the hackers “maintaining access and footholds within some victim IT environments for at least five years”. The statement, which was co-signed by the respective cybersecurity agencies of Britain, Australia, Canada and New Zealand, is the latest in a series of warnings from US officials about Volt Typhoon, a group that has drawn particular alarm because it appears geared toward sabotage rather than espionage. The widespread nature of the hacks has led to a series of meetings between the White House and the private technology industry, including several telecommunications and cloud computing companies, in which the US government asked for assistance in tracking the activity. “We are extraordinarily concerned about malicious cyber activity from the PRC state-sponsored actor that industry calls Volt Typhoon,” a senior CISA official, Eric Goldstein, referring to the People’s Republic of China, told Reuters ahead of the statement’s release. “Most of the victims we have identified have no legitimate espionage value.”