Explainer: what is Volt Typhoon and why is it the ‘defining threat of our generation’?

Publication Date: 2024-02-13

Author: Helen Davidson

Section: Technology

Tags: Hacking, China, explainers

Article URL: https://www.theguardian.com/technology/2024/feb/13/volt-typhoon-what-is-it-how-does-it-work-chinese-cyber-operation-china-hackers-explainer

Relations between the US and China – particularly over Beijing’s threats to annex Taiwan – have plummeted in recent years, prompting growing concern about the potential for hostilities or all-out conflict. So recent revelations that a Chinese hacking network known as Volt Typhoon had been lying dormant inside US critical infrastructure for as long as five years have sparked considerable alarm. The network exploited US technological and security weaknesses. But rather than stealing secrets, US and allied intelligence services said it was focused on “pre-positioning” itself for future acts of sabotage. FBI director Christopher Wray told a US committee hearing last week that Volt Typhoon was “the defining threat of our generation”. The Netherlands and Philippines have also recently publicly identified Chinese-backed hackers as targeting state networks and infrastructure. What is Volt Typhoon? Western intelligence officials say Volt Typhoon – also known as Vanguard Panda, Brronze Silhouette, Dev-0391, UNC3236, Voltzite, and Insidious Taurus – is a state-supported Chinese cyber operation that has compromised thousands of internet-connected devices. They said it was part of a larger effort to infiltrate western critical infrastructure, including naval ports, internet service providers, communications services and utilities. The new advisories on Volt Typhoon followed a recent announcement by US authorities that they had dismantled a bot network of hundreds of compromised devices, attributing it to the hacking network. “CISA [Cybersecurity and Infrastructure Agency] teams have found and eradicated Chinese intrusions in multiple critical infrastructure sectors, including aviation, water, energy, [and] transportation,” US CISA director Jen Easterly told a US House committee hearing earlier this month. How does it work? Volt Typhoon works by exploiting vulnerabilities in small and end-of-life routers, firewalls and virtual private networks (VPNs), often using administrator credentials and stolen passwords, or taking advantage of outmoded tech that hasn’t had regular security updates – key weaknesses identified in US digital infrastructure. It uses “living off the land” techniques, whereby malware only uses existing resources in the operating system of what it’s targeting, rather than introducing a new (and more discoverable) file. A report released last week by CISA, the National Security Agency, and the FBI, said Volt Typhoon hackers had maintained this access for the past five years, and while it has targeted only US infrastructure, the infiltration was likely to have affected the US’s “Five Eyes” allies of Canada, Australia, New Zealand, and the UK. What is its aim? US authorities said Volt Typhoon’s unusual choice of targets and behavioural patterns were not consistent with traditional cyber espionage or intelligence gathering operations. Volt Typhoon has been active since mid-2021, according to a Microsoft investigation published last year. Targeting US infrastructure in Guam and elsewhere, Microsoft found it had been “pursuing development of capabilities that could disrupt critical communications infrastructure between the United

States and Asia region during future crises". "People's Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against US critical infrastructure in the event of a major crisis or conflict with the United States," said the joint report. What does China say? Beijing routinely denies any accusations of cyber-attacks and espionage linked to or backed by the Chinese state. But evidence of Beijing's cyber-espionage campaigns has been building for more than two decades. Spying has come into sharp focus over the past 10 years as western researchers tied breaches to specific units within the People's Liberation Army, and US law enforcement charged a string of Chinese officers with stealing American secrets. Secureworks, an arm of Dell Technologies, said in a blog post last year that Volt Typhoon's interest in operational security likely stemmed from embarrassment over the drumbeat of US indictments and "increased pressure from (Chinese) leadership to avoid public scrutiny of its cyber-espionage activity". What's next? 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. Institutions and assets targeted by the now dismantled botnet were ordered by CISA in January to disconnect affected devices and products, starting off an intensive and difficult process of remediation. "This was necessary given the degree of targeting and compromise around the world of the now three exploited vulnerabilities affecting these appliances," Eric Goldstein, CISA's executive assistant director for cybersecurity, told the Risky Business podcast. "Every organisation running these devices absolutely needs to assume targeting and assume compromise."