China Accuses U.S. of Fabricating Volt Typhoon to Hide Its Own Hacking Campaigns

By The Hacker News

Published: 2024-10-15 · Archived: 2026-04-05 20:11:30 UTC

China's National Computer Virus Emergency Response Center (CVERC) has doubled down on claims that the threat actor known as Volt Typhoon is a fabrication of the U.S. and its allies.

The agency, in collaboration with the National Engineering Laboratory for Computer Virus Prevention Technology, went on to accuse the U.S. federal government, intelligence agencies, and Five Eyes countries of conducting cyber espionage activities against China, France, Germany, Japan, and internet users globally.

It also said there's "ironclad evidence" indicating that the U.S. carries out false flag operations in an attempt to conceal its own malicious cyber attacks, adding it's inventing the "so-called danger of Chinese cyber attacks" and that it has established a "large-scale global internet surveillance network."

"And the fact that the U.S. adopted supply chain attacks, implanted backdoors in internet products and 'pre-positioned' has completely debunked the Volt Typhoon – a political farce written, directed, and acted by the U.S. federal government," it said.

"The U.S. military base in Guam has not been a victim of the Volt Typhoon cyber attacks at all, but the initiator of a large number of cyberattacks against China and many Southeast Asian countries and the backhaul center of stolen data."

It's worth noting that a previous report published by CVERC in July characterized the Volt Typhoon actor as a misinformation campaign orchestrated by the U.S. intelligence agencies.

Volt Typhoon is the moniker assigned to a China-nexus cyber espionage group that's believed to be active since 2019, stealthily embedding itself into critical infrastructure networks by routing traffic through edge devices comprising routers, firewalls, and VPN hardware in an effort to blend in and fly under the radar.

As recently as late August 2024, it was linked to the zero-day exploitation of a high-severity security flaw impacting Versa Director (CVE-2024-39717, CVSS score: 6.6) to deliver a web shell named VersaMem for facilitating credential theft and run arbitrary code.

The use of edge devices by China-linked intrusion sets has become something of a pattern in recent years, with some campaigns leveraging them as Operational Relay Boxes (ORBs) to evade detection.

This is substantiated by a recent report published by French cybersecurity company Sekoia, which attributed threat actors likely of Chinese origin to a wide-range attack campaign that infects edge devices like routers and cameras to deploy backdoors such as GobRAT and Bulbature for follow-on attacks against targets of interest.

"Bulbature, an implant that was not yet documented in open source, seems to be only used to transform the compromised edge device into an ORB to relay attacks against final victims networks," the researchers said.

"This architecture, consisting of compromised edge devices acting as ORBs, allows an operator to carry out offensive cyber operations around the world near to the final targets and hide its location by creating on-demand proxies tunnels."

In the latest 59-page document, Chinese authorities said more than 50 security experts from the U.S., Europe, and Asia reached out to the CVERC, expressing concerns related to "the U.S. false narrative" about Volt Typhoon and the lack of evidence linking the threat actor to China.

The CVERC, however, did not name those experts, nor their reasons to back up the hypothesis. It further went on to state that the U.S. intelligence agencies created a stealthy toolkit dubbed Marble no later than 2015 with the intent to confuse attribution efforts.

"The toolkit is a tool framework that can be integrated with other cyber weapon development projects to assist cyber weapon developers in obfuscating various identifiable features in program code, effectively 'erasing' the 'fingerprints' of cyber weapon developers," it said.

"What's more, the framework has a more 'shameless' function to insert strings in other languages, such as Chinese, Russian, Korean, Persian, and Arabic, which is obviously intended to mislead investigators and frame China, Russia, North Korea, Iran, and Arab countries."

The report further takes the opportunity to accuse the U.S. of relying on its "innate technological advantages and geological advantages in the construction of the internet" to control fiber optic cables across the Atlantic and the Pacific and using them for "indiscriminate monitoring" of internet users worldwide.

It also alleged that companies like Microsoft and CrowdStrike have resorted to giving "absurd" monikers with "obvious geopolitical overtones" for threat activity groups with names like "typhoon," "panda," and "dragon."

"Again, we would like to call for extensive international collaboration in this field," it concluded. "Moreover, cybersecurity companies and research institutions should focus on counter-cyber threat technology research and better products and services for users."

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
