Beijing accused of misusing Western research to claim Volt Typhoon is a ransomware group

By Alexander Martin

Published: 2024-07-10 · Archived: 2026-04-02 10:58:44 UTC

China's national cybersecurity agency was accused on Wednesday of misrepresenting research from Western cybersecurity companies in an ongoing attempt to deny allegations that a Being-backed hacking group is behind attacks targeting critical infrastructure in the West.

The cybersecurity company Trellix pushed back against a conspiratorial report published Monday by China's National Computer Virus Emergency Response Center (CVERC) claiming that the Five Eyes intelligence alliance had concocted evidence about the hacking campaign.

"This is likely an effort from the Chinese government to manipulate public perceptions of China threats," said John Fokker, the head of threat intelligence at Trellix.

As researchers previously told Recorded Future News, the group tracked as Volt Typhoon by Microsoft and as Bronze Silhouette by Secureworks has gone to great lengths to conceal its connections to China, suggesting that Beijing has become increasingly sensitive about being blamed for offensive cyber operations.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) had in February warned that the hackers were "seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States."

It was shortly after this warning that the CVERC, alongside the English-language version of the Global Times newspaper — controlled by the Chinese Communist Party — first claimed that the threat actor does not exist.

In the CVERC report published on Monday, coordinated with another article in the Global Times, the Chinese agency claimed that Volt Typhoon was a "misinformation campaign" intentionally misattributing cyberattacks by the Dark Power ransomware group to the Chinese state.

The CVERC report includes a number of grammatical and spelling errors, even of Chinese institutions — in one case calling the military-linked Northwestern Polytechnical University the Northwestern Pyrotechnical University — and according to Dakota Cary, a consultant at SentinelOne, was potentially "co-authored by the propagandists at Global Times."

In its substance, the report misrepresents the vocabulary of intelligence analysis to claim there are disagreements between intelligence assessments made by CISA and private sector cybersecurity companies about activities linked to this hacking group.

In one instance, the CVERC cited Mandiant using estimative language about a cluster of activity tracked as UNC5291 which Mandiant assessed "with medium confidence to be Volt Typhoon, targeting U.S. energy and

defence sectors."

Mandiant said that it had seen the UNC5291 campaign probe "Ivanti Connect Secure appliances in mid-January 2024," but had "not directly observed Volt Typhoon successfully compromise Ivanti Connect Secure."

This was taken to contradict a CISA's warning that the group had been exploiting vulnerabilities in networking appliances, including Ivanti Connect Secure, rather than simply a statement of Mandiant's own observations.

In another instance the CVERC cited reports by Trellix and ThreatMon which included among their indicators of compromise the hash of a ransomware sample from the Dark Power group, a sample which it claimed was connected with IP addresses also linked to Volt Typhoon.

Fokker said the CVERC report "uses our blog to support a false conclusion that there is a connection between Dark Power and Volt Typhoon, which our research does not substantiate."

Neither Mandiant nor ThreatMon were able to respond to requests for comment before publication. Numerous other cybersecurity companies have also reported incidents attributed to Volt Typhoon in which the threat actor has targeted critical infrastructure in the United States, including Bitdefender, Secureworks, Microsoft and others.

Alexander Martin

is the UK Editor for Recorded Future News. He was previously a technology reporter for Sky News and a fellow at the European Cyber Conflict Research Initiative, now Virtual Routes. He can be reached securely using Signal on: AlexanderMartin.79
