

Chinese cyber agency accused of 'false and baseless' claims about US interfering in Volt Typhoon research

By Alexander Martin

Published: 2024-07-11 · Archived: 2026-04-02 12:45:22 UTC

China's national cybersecurity agency was accused on Thursday of falsely claiming, citing an "anonymous" inside source, that a Western threat intelligence company had "recalled" a publication under pressure from an unidentified U.S. intelligence agency.

U.S.-based ThreatMon said China's National Computer Virus Emergency Response Center (CVERC) completely mischaracterized the company's changes to a report on the Dark Power ransomware group.

It's the latest pushback from a Western company against [a conspiratorial report](#) that the CVERC published Monday, in which it attempted to deny that a Beijing-backed hacking group was behind attacks targeting critical infrastructure in the West.

The CVERC argued that the China state-sponsored threat actor Volt Typhoon was an invention of Western intelligence agencies. It claimed that any real attacks that had taken place were instead conducted by the Dark Power ransomware gang, and that evidence revealing this was being suppressed.

It attempted to justify the claims of this conspiracy by citing reports from ThreatMon and Trellix, another U.S.-based cybersecurity company.

The agency noted that ThreatMon had once published and then amended a report about Dark Power that included several Indicators of Compromise (IoCs) — digital forensics artifacts shared by cybersecurity defenders to uncover and attribute hacks — which Trellix had linked to Volt Typhoon.

Citing an "anonymous source" from ThreatMon — the first time a report from the CVERC has presented alleged human intelligence — the agency claimed that ThreatMon had removed the indicators of compromise (IoCs) linked to Dark Power from the amended version of its report after being "manipulated by intelligence agencies."

Gökhan Yüceler, the chief technology officer at ThreatMon, told Recorded Future News that "the allegations that we are acting under pressure from the U.S. are entirely false and baseless."

Yüceler said that the company removed the IoCs from its amended Dark Power report after subsequent analysis suggested they may be incorrect.

"The recent report from China aims to misrepresent our research. The report claims a connection between Volt Typhoon and Dark Power based on our findings, a connection our research does not support. While shared IoCs can occur, drawing definitive conclusions from them is misleading," he said.

The cybersecurity company Trellix also [pushed back](#) against the CVERC’s claims. John Fokker, the company’s head of threat intelligence, told Recorded Future News 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.

“This is likely an effort from the Chinese government to manipulate public perceptions of China threats,” Fokker said.

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. The CVERC’s most recent report was again accompanied by [another article](#) in the Global Times.

The 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. According to Dakota Cary, a consultant at SentinelOne, the report was potentially “co-authored by the propagandists at Global Times.”

 Recorded Future®

Know what matters.

Act first.

Get started





[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

Source: <https://therecord.media/china-cyber-agency-claims-us-interference-volt-typhoon-research>