Mandiant Intelligence Chief Raises Alarm Over China's 'Volt Typhoon' Hackers in US Critical Infrastructure

By Ryan Naraine

Published: 2023-10-25 · Archived: 2026-04-05 16:35:56 UTC

ATLANTA – SECURITYWEEK 2023 ICS CYBERSECURITY CONFERENCE – Chief analyst at Mandiant Intelligence John Hultquist says defenders in the critical infrastructure trenches should urgently work on finding and removing traces of Volt Typhoon, a Chinese government-backed hacking team caught in a series of eyebrow-raising attacks against targets in Guam and the United States.

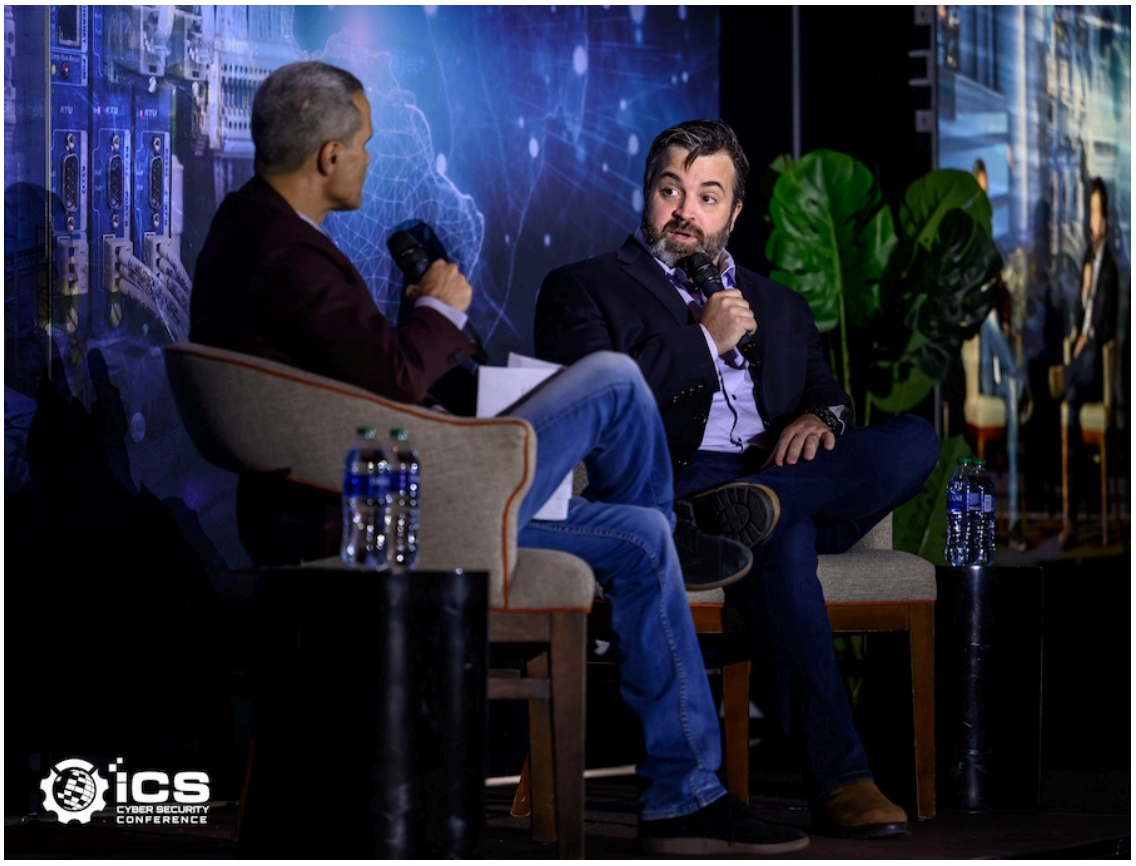
Speaking at a keynote fireside chat at SecurityWeek's 2023 ICS Cybersecurity Conference in Atlanta on Tuesday, Hultquist said the Volt Typhoon campaign included "very deliberate targeting of critical infrastructure" installations and represents a major shift by Chinese hacking teams known mostly for economic espionage and IP theft.

"This Volt Typhoon activity is a brand-new thing for them. We have not seen a lot of deliberate targeting in the critical infrastructure space from China," Hultquist said. "Occasionally, we'll catch them probing into power, but this is a deliberate, long-term attempt to infiltrate a lot of critical infrastructure in a way that stays below the radar."

The Volt Typhoon campaign was first flagged by Microsoft with deliberate targeting of critical infrastructure in Guam, a discovery that raised eyebrows because the tiny island is considered an important part of a future China/Taiwan military conflict.

"They were found in Guam but they were also discovered all over the continental United States, including in telecommunications and logistics. Microsoft indicated that they've also been found in power and water sectors," Hultquist noted.

"The NSA indicated that their theory behind this is that they are digging in for the possibility of creating a disruptive event in the event of a wartime scenario. While I don't have the intelligence to confirm that, the deliberate targeting of critical infrastructure makes it a priority for us. This is especially concerning given how hard they're working on their operational security, using botnets and zero-days to stay below the radar," Hultquist added.



Volt Typhoon has been publicly documented as "stealthy and targeted malicious activity focused on post-compromise credential access and network system discovery."

"Microsoft assesses with moderate confidence that this [Chinese cyberespionage] campaign is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises," the software giant said in a note documenting the APT discovery.

The group, active since mid-2021, has compromised a wide variety of organizations spanning communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and the education sectors.

Hultquist urged defenders to prioritize patching and mitigations for internet-facing edge devices and network routers that provide a major entry point for high-end attackers.

In the case of Volt Typhoon, he noted that the attackers are leveraging botnets for command and control with minimal use of malware, making it really hard to hunt them.

“You should really be keeping your eye on two things right now. One is the Volt Typhoon situation; it’s all over the United States. They are clearly dug in, and we’re going to have to root them out. The second one is the current situation in the Middle East. The United States is heavily involved, and because of that, the likelihood of some sort of response, possibly from Iran, is legitimate. We have to keep that in mind as well. You’re starting to see some telemetry; they are at play without a doubt.”

Sessions from SecurityWeek’s ICS Cybersecurity Conference can be watched in both live stream and on demand this week.

Related: AWS Using MadPot Decoy System to Disrupt APTs, Botnets

Related: Microsoft Says Chinese .Gov Hackers Targeting US Critical Infrastructure

Related: Fortinet Warns of Possible Zero-Day Exploited in Limited Attacks

---