China's Volt Typhoon APT Burrows Deeper Into US Critical Infrastructure

By Nate Nelson

Published: 2023-07-31 · Archived: 2026-04-05 22:47:40 UTC

4 Min Read

Source: RGB Ventures/SuperStock via Alamy Stock Photo

The US military was reckoning with two major cyber concerns over the weekend — one the widespread and still unresolved Chinese campaign known as Volt Typhoon targeting military bases, and the other an insider breach affecting Air Force and FBI communications.

Biden administration officials have confirmed that Volt Typhoon's malware is much more endemic than previously thought; responders have found it planted inside numerous networks controlling the communications, power, and water feeding US military bases at home and abroad, according to The New York Times.

Also concerning, those same networks also touch run of the mill businesses and individuals as well — and investigators are having a hard time assessing the full footprint of the infestation.

Meanwhile, a search warrant obtained by Forbes revealed that the Pentagon is dealing with a wholly separate cyber intrusion — in this case, a communications compromise affecting 17 Air Force facilities, and possibly the FBI as well, courtesy of an Air Force engineer.

Chinese Malware a 'Ticking Time Bomb' Inside Critical US Networks

The Chinese state-aligned advanced persistent threat (APT) behind Volt Typhoon, aka "Vanguard Panda," came to attention after Microsoft observed Chinese cyber activity in Guam, the site of a US military base strategically significant to the defense of Taiwan against Chinese aggression. Microsoft posited at the time "that this Volt Typhoon campaign is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises."

That case, disclosed in May, has turned out to be just one small part of a much broader campaign, and the aim towards being in place to carry out destruction now seems increasingly likely as a motivation; sources told the Times that the attackers are in a position to handicap military response and supply chains for materiel should a kinetic conflict kick off.

"More than a dozen US officials and industry experts said in interviews over the past two months that the Chinese effort goes far beyond telecommunications systems and predated the May report by at least a year," the New York Times reported July 29, with one congressman pithily labeling the campaign "a ticking time bomb."

Further, the Times reported that "There is a debate inside the administration over whether the goal of the operation is primarily aimed at disrupting the military, or at civilian life more broadly in the event of a conflict."

Austin Berglas, a former FBI Cyber Division special agent, now global head of professional services at BlueVoyant, isn't surprised that China is buried inside of the US's most critical networks.

"We've known that China is looking to exploit any sector it could to give them an advantage politically, socially, or economically. So it's not surprising," he says. "What is surprising is the mention of destructive malware. That's not normally seen in their typical toolkit."

"When you look at traditional tactics, techniques, and procedures (TTPs) used by Chinese state actors, they're doing espionage," he explains. Malware designed to disrupt or destroy critical systems changes the story. "Is it positioning them for a retaliatory strike? Is it something that we're going to start seeing more of in the future from these guys?"

An Insider Attack Takes Flight at the Air Force

Also on July 29, Forbes revealed that the Pentagon ordered a raid on a 48-year-old engineer from the Arnold Air Force base in Tullahoma, Tenn.

According to the relevant search warrant, the engineer had taken $90,000 worth of radio equipment home, gaining unauthorized access to radio communications technologies employed by Air Education and Training Command (AETC), a wing of the Air Force responsible for recruitment and training.

In the raid, investigators found an open computer running a Motorola radio programming software "which contained the entire Arnold Air Force Base (AAFB) communications system," the warrant stated, plus evidence of access to privileged communications from the FBI and other Tennessee state agencies.

Berglas says that the impact on the other agencies is not surprising. He likens it to his time in the FBI. "If I was sitting at my desk at work, I couldn't put a USB drive into my computer. I couldn't put a disc in to make a copy, or take that media off of the network any other way, aside from printing," he explains.

"The problem is, as an FBI office, you rely heavily on state and local partners. So you need to give them classified access to certain levels of information, depending on the investigation. But when that information gets to that office, those task forces and contractors probably don't have the same level of cyber safeguards in place," he explains.

It's a lesson for any organization: Even those that practice such stringent zero trust as the FBI and Air Force still face the same insider threats, and the same supply chain risks, as any other organization.

"When you're looking at securing classified information," he concludes, "you have to enable those individual and agency partners to comply. It's about giving resources to the weakest link in the chain, and supporting them to be more secure."

About the Author

Contributing Writer

Nate Nelson is a journalist and scriptwriter. He writes for "Darknet Diaries" — the most popular podcast in cybersecurity — and co-created the former Top 20 tech podcast "Malicious Life." Before joining Dark Reading,

he was a reporter at Threatpost.
