China-Backed Hackers Threaten Texas Military Sites, Utilities

govtech.com/security/china-backed-hackers-threaten-texas-military-sites-utilities

July 31, 2023

Shutterstock

(TNS) — A Chinese government-backed hacker group's apparent plan to upend utilities and communication systems that power U.S. military bases poses a major threat to Joint Base San Antonio — and potentially to the region's water and electricity customers.

U.S. officials say the group, called Volt Typhoon, has inserted malware — computer code intended to damage or disrupt networks or to covertly collect information — deep in the systems of numerous water and electric utilities that serve military installations in the United States and abroad.

The aim could be to delay a U.S. military response if China's People's Liberation Army invades Taiwan. President Joe Biden has said the U.S. military would intervene if China invaded the island nation.

"I would be most concerned about U.S. assets in the Pacific Rim — in South Korea and Japan," said John Dickson, a San Antonio-based cybersecurity consultant and former Air Force intelligence officer. "But we are Military City, USA, and a sophisticated reader doesn't have to do too much to connect the dots."

San Antonio is flush with military personnel and missions. It's home to Fort Sam Houston, the largest military medical training installation in the U.S., as well as to JBSA-Randolph and JBSA-Lackland Air Force bases.

Lackland trains the service's incoming airmen and conducts cyber warfare and intelligence-gathering operations at its Security Hill facility.

The National Security Agency's Texas Cryptologic Center occupies a sprawling campus on San Antonio's West Side. The center conducts worldwide signals intelligence and cybersecurity operations. Signals intelligence involves collecting, decoding and interpreting electronic communications.

It's unclear if the networks of the San Antonio Water System or CPS Energy, both owned by the city of San Antonio, are infected with Volt Typhoon's malware.

CPS, the largest municipally owned utility in the U.S., has 930,000 electric and 381,000 gas customers. SAWS serves 511,000 water and 456,000 wastewater customers. The two utilities' service areas encompass Bexar County and small swaths of neighboring counties.

"We will continue to monitor this threat," CPS officials said in a statement. "We won't comment further on security risks to the military."

In 2019, the electric utility took ownership of the electric and natural gas infrastructure at Lackland and Randolph under a 50-year, $289 million contract with the Defense Logistics Agency, an arm of the Defense Department. CPS is responsible for operating and maintaining the bases' power systems.

Gavino Ramos, SAWS' senior vice president of communications and external affairs, declined to comment on the hacking threat "due to security reasons." However, he noted that "SAWS provides some bases with retail and wholesale water/wastewater services."

In 2015, SAWS officials signed an agreement to supply Joint Base San Antonio installations with a "redundant," or backup, water source.

The utility's financial report for 2022 shows that Lackland and Fort Sam Houston were the largest and second-largest wholesale wastewater customers among government entities in SAWS' service area. The Lackland Training Annex was No. 9 on the list.

"I'm sure CPS and SAWS are looking for the malware on their networks," said Max Kilger, a cybersecurity expert and professor at the University of Texas at San Antonio's School of Data Science. "CPS is actually pretty forward-looking in these matters."

Federal authorities don't have the wherewithal to scour the network of every organization that serves U.S. military bases. The U.S. government is likely helping the two San Antonio utilities hunt for the malicious computer code, providing "hints, clues and intel," Kilger said.

"The Department of Homeland Security will assist and say, 'We've seen this kind of traffic coming out of affected organizations — you should look for similar activity,' " said Kilger, who is director of Critical Technologies Studies at UTSA.

How such a cyber attack would affect SAWS and CPS customers is unknown.

"The worst-case scenario is the power grid goes down," Kilger said. "It's incredibly serious if it's long-lasting and widespread."

'STEALTHY AND MALICIOUS'

Microsoft sounded the warning about Volt Typhoon's malware in a blog post May 24, saying it had detected "stealthy and targeted malicious activity" targeting "critical infrastructure organizations" in the United States.

The software giant said Volt Typhoon "typically focuses on espionage and information gathering."

"Volt Typhoon has been active since mid-2021 and has targeted critical infrastructure organizations in Guam and elsewhere in the United States," Microsoft said. "In this campaign, the affected organizations span the communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors."

The hacker activity targeting Guam is significant because the Pacific island is home to Anderson Air Force Base.

On the same day as the Microsoft blog post, the U.S. Cybersecurity and Infrastructure Security Agency issued an advisory about Volt Typhoon, saying the Chinese government-sponsored hackers were active "across U.S. critical infrastructure sectors."

The New York Times reported Saturday that the Biden administration was trying to hunt down the malicious code and that the problem has been the subject of Situation Room meetings in the White House involving senior officials from the National Security Council, the Pentagon, the Homeland Security Department and the nation's spy agencies.

Although cybersecurity experts may be taken aback by the scale of the malware infiltration, they weren't surprised by it.

"I've always assumed that they — nation-states, specifically China — have hooks into our systems," Dickson said.