Take Action: Scan Your Utility Networks for China State-Sponsored Cyber Attackers

Summary

Water and wastewater systems remain at high risk of becoming victims of Volt Typhoon (also known as BRONZESILHOETTE and VANGUARD PANDA), a People's Republic of China (PRC) state-sponsored cyber actor. System owners and operators should direct their network administrators to review this CSA and carry out the recommended mitigation procedures listed below. New information has been discovered on Volt Typhoon's network scanning and other reconnaissance activities at US entities in the energy, aviation, and defense sectors as recently as mid-June 2023. Network scanning and reconnaissance activities can allow a threat actor to gain information about a target's network and use that information to identify potential vulnerabilities to launch a future attack.

Indicators of Compromise

Indicators of Compromise (IOC) are pieces of digital evidence that suggests a network may have been breached. Volt Typhoon has previously used the below IP addresses and User-Agent string to conduct reconnaissance activities (Note: This list is not comprehensive and absence of hits should not be viewed as definitive):

43.11.3.120	109.166.39.179
45.11.3.147	185.126.226.179
45.11.3.191	185.171.120.209
45.32.175.202	208.83.239.166
45.76.173.220	216.128.137.135
108.61.192.179	User-agent of Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/5/37.36 (KHTML, like gecko) chrome/102.0.0.0 Safari/537.36
108.61.252.58	
109.166.39.177	

Mitigation

Water and wastewater system owners and operators should direct their network administrators to review the CSA, along with the indicators of compromise included in this alert, and carry out the recommended mitigation procedures below. Volt Typhoon, among many other PRC APT groups, uses dynamic infrastructure and preinstalled, legitimate tools in victim environments to conduct their cyber activities. The CSA provides the most comprehensive and enduring detection mitigation measures to help network administrators in searching for this activity.

- Scan your network for the known indicators of compromise included in this alert, and other unusual IP addresses and ports in command lines, registry entries, and firewall logs to identify other hosts that are potentially involved in actor actions.
- Block all listed IP addresses and user-agents listed in this updated alert.
- Establish baselines of normal activity, particularly for remote access and administrative actions, and look for outliers from those baselines.

The U.S. EPA Office of Water request recipients to pass along this alert to all Water & Wastewater entities. If you have questions about any of the information contained in this document, please contact Brandon Carter, Water Infrastructure and Cyber Resilience Division, USEPA (carter.brandon@epa.gov). If you find evidence of potential Volt Typhoon activity, please report this activity to FBI at Internet Crime Complaint Center (IC3) | File a Complaint or CISA at Incident Reporting System | CISA.