NARUC
National Association of
Regulatory Utility Commissioners

Cybersecurity Emerging Issue Brief

Volt Typhoon

On February 7, 2024, multiple federal agencies released a joint advisory detailing a China-backed cyber threat actor group named Volt Typhoon, which is known to have compromised IT environments of multiple critical infrastructure sectors — primarily Communications, Energy, Transportation, and Water and Wastewater systems — in the United States and U. S. territories. The advisory assesses with high confidence that the Volt Typhoon actors are pre-positioning themselves on Information Technology networks to enable lateral movement to Operational Technology (OT) assets for the purpose of disrupting critical functions in the event of conflict between China and the U.S.

Volt Typhoon has a strong focus on stealth. This indicates that their aim is to achieve and maintain persistence on compromised networks, employing tactics known as "Living off the Land (LOTL)," to evade detection. LOTL involves the abuse of legitimate tools and processes on compromised systems to blend in with normal activities and operate discreetly without being detected. To gain initial access to a victim environment, Volt Typhoon leverages both zero-day and known vulnerabilities in internet-facing networking appliances such as firewalls and Virtual Private Networks.

The joint advisory contains several mitigation recommendations for Critical infrastructure organizations and their technology manufacturers:

- Apply patches for internet-facing systems and prioritize the patching of critical vulnerabilities in appliances known to be frequently exploited by Volt Typhoon.
- Implement phishing-resistant multi-factor authentication (MFA) security measures.
- Ensure logging is turned on for application, access, and security logs and store logs in a central system.

PUCs interested in gaining a better understanding of Volt Typhoon tactics, techniques, and practices and the actions that utilities are taking in response, might ask the following questions of their jurisdictional utilities:

- Have you conducted comprehensive risk assessments to identify vulnerabilities in IT and operational technology (OT) systems?
- Have you patched critical vulnerabilities, especially those known to have been exploited by Volt Typhoon? If not, why not and what is the timeline for doing so?
- Is phishing-resistant, multi-factor authentication applied to critical systems?
- Have application, access, and security logs for IT and OT systems been examined for signs of Volt Typhoon infiltration and living off the land abuses to hide their presence?
- Do configuration baselines exist, particularly in OT networks, so comparisons may be made to the current-state environment and anomalies detected?
- Does a detailed cyber incident response plan exist and include, for example, steps to reset user and privileged account access? If so, when was the last time the plan was tested?
- How are you engaging with third-party vendors and suppliers critical to utility operations to assess their vulnerabilities to Volt Typhoon's known tactics, techniques and procedures?
- Are you monitoring ISACs and CISA websites for updates on Volt Typhoon's tactics, techniques, and practices and applying additional mitigations as they become available?

Additional Resources:

This brief is intended for Public Utility Commission audiences. Please refer to official CISA, DOE, FBI, and other guidance for technical details.

- CISA Advisory: https://www.cisa.gov/news-events/alerts/2023/05/24/cisa-and-partners-release-cybersecurity-advisory-guidance-detailing-prc-state-sponsored-actors.
- CISA Alert: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a
- Joint advisory Technical Approaches to Uncovering and Remediating Malicious Activity.
- CISA Secure by Design Alert: https://www.cisa.gov/sites/default/files/2024-01/SbD-Alert-Security-Design-Improvements-for-SOHO-Device-Manufacturers.pdf
- CISA's Secure by Design website.
- Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. Although tailored to U.S. Federal Civilian Executive Branch (FCEB) agencies, the playbooks are applicable to all organizations. The incident response playbook provides procedures to identify, coordinate, remediate, recover, and track successful mitigations from incidents.
- Joint Water and Wastewater Sector - Incident Response Guide. This joint guide provides incident response best practices and information on federal resources for Water and Wastewater Systems Sector organizations.

Acknowledgment: This material is based upon work supported by the Department of Energy under Award Number DE-CR0000009.

February 21, 2024