TLP:CLEAR

PRC State-Sponsored Actors Use BRICKSTORM Malware for Long-Term Persistence on Victim Systems

The U.S. EPA is issuing this alert to inform drinking water and wastewater system owners and operators about recent cyber-threat activity involving state-sponsored actors from the People's Republic of China (PRC). PRC threat actors are deploying BRICKSTORM malware to maintain long-term persistence on victims' systems. BRICKSTORM is a sophisticated backdoor capable of exploiting and operating in VMware Sphere systems as well as Windows systems, enabling threat actors to sustain stealthy access and providing capabilities for initiation, persistence, and secure command-and-control operations. BRICKSTORM can conceal its malicious communications and facilitate lateral movement from IT to OT networks by creating hidden, encrypted pathways within the victims' networks, making it difficult to detect. Additionally, it utilizes a self-monitoring function that automatically reinstalls or restarts the malware if disrupted with a goal of continued operation.

Mitigations

All drinking water and wastewater systems operating VMware vSphere and Windows environments are strongly encouraged to implement the following mitigations immediately to enhance resilience against the BRICKSTORM malware. Systems that outsource technology support should consult with their service providers for assistance with these steps:

- Upgrade VMware vSphere servers to the latest version.
- Take inventory of all network edge devices and monitor for any suspicious network connectivity originating from these devices.
- Ensure proper network segmentation restricts network traffic from the DMZ to the internal network.
- Disable Remote Desktop Protocol and Server Message Block from the DMZ to the internal network.
- Apply the principle of least privilege and restrict service accounts to only needed permissions.
- Increase monitoring for service accounts, which are highly privileged and have a predictable pattern of behavior.
- Block unauthorized DNS-over-HTTPS (DoH) providers and external DoH network traffic to reduce unmonitored communications.
- Scan for BRICKSTORM using CISA-created YARA and Sigma rules found here: CISA BRICKSTORM YARA Rules.

- CISA requests that organizations report BRICKSTORM, similar malware, or potentially related activity to CISA's 24/7 Operations Center (contact@cisa.dhs.gov), 1-844-Say-CISA (1-844-729-2472), or CISA's Incident Reporting System. Please identify the activity is related to BRICKSTORM, and CISA will reach out with next steps.

Conclusion

For additional details please refer to CISA alert AR25-338A: BRICKSTORM Backdoor. If you have questions about any of the information in this alert, including assistance with the mitigation steps, please submit a request to EPA's Cybersecurity Technical Assistance Program for the Water Sector.