VOLTZITE | Dragos

dragos.com/threat/voltzite/

February 16, 2024

Threat Group

VOLTZITE

Active Since 2023

VOLTZITE traditionally targets US-based facilities, but also known to target organizations in Africa and Southeast Asia, using LOTL techniques that make detection and response difficult.

VOLTZITE, a Dragos-tracked threat group that has operational overlaps with Volt Typhoon (Microsoft), was performing reconnaissance and enumeration of multiple US-based electric companies, and since then has been observed targeting electric power transmission and distribution, emergency services, telecommunications, defense industrial bases, and satellite services. VOLTZITE's actions towards US electric entities, telecommunications, and GIS systems signify clear objectives to identify vulnerability within the country's critical infrastructure that can be exploited in the future with destructive or disruptive cyber attacks. While VOLTZITE has traditionally targeted US facilities, we also are aware of the group targeting organizations in Africa and Southeast Asia.

This group heavily uses living off the land (LOTL) techniques, which can make detection

and response efforts more difficult. This strategy, paired with slow and steady reconnaissance, enables VOLTZITE to avoid detection from security teams.

VOLTZITE's 2023 behavior suggested operational objectives of espionage and information gathering. Data stolen from operational technology (OT) networks may result in unintended disruption to critical industrial processes or provide the adversary with crucial intelligence to aid in follow-up offensive tool development or attacks against ICS networks.

About Dragos Threat Intelligence

Dragos threat intelligence leverages the Dragos Platform, our threat operations center, and other sources to provide comprehensive insight into threats affecting industrial control security and safety worldwide. Dragos does not corroborate nor conduct political attribution to threat activity. Dragos instead focuses on threat behaviors and appropriate detection and response. Read more about Dragos's approach to categorizing threat activity and attribution.

Dragos does not publicly describe ICS threat group technical details except in extraordinary circumstances in order to limit tradecraft proliferation. However, full details on VOLTZITE and other group tools, techniques, procedures, and infrastructure are available to network defenders via Dragos WorldView.