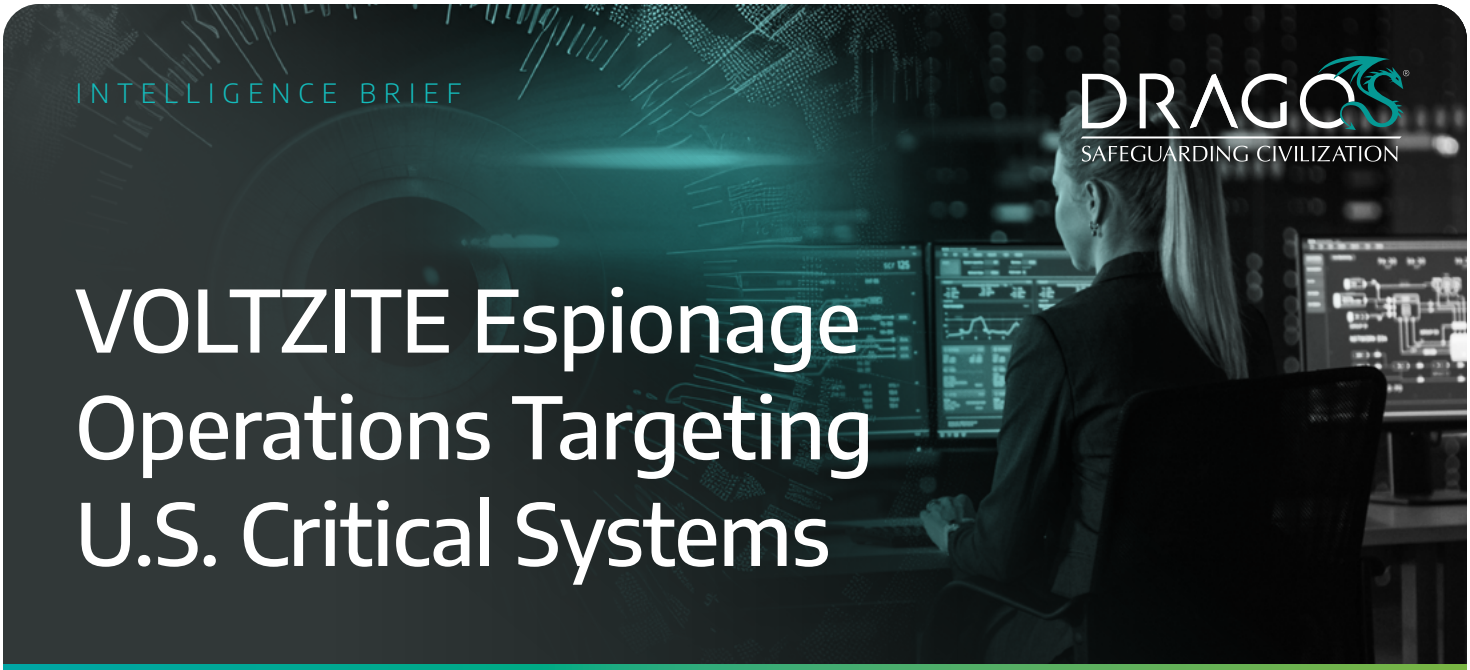
INTELLIGENCE BRIEF



VOLTZITE Espionage Operations Targeting U.S. Critical Systems

JOSH HANRAHAN | PRINCIPAL ADVERSARY HUNTER

DRAGOS, INC

FEBRUARY 2024

Summary

VOLTZITE is a Dragos designated threat group. This threat group shares overlaps with the adversary described by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) in May 2023, and the Microsoft threat group Volt Typhoon. VOLTZITE has been observed performing reconnaissance and enumeration of multiple U.S.-based electric companies since early 2023, and since then has targeted emergency management services, telecommunications, satellite services, and defense industrial bases. Additionally, Dragos has discovered VOLTZITE targeting electric transmission and distribution organizations in African nations. VOLTZITE employs living off the land (LOTL) techniques; they use native tools available in compromised assets. This strategy, paired with slow and steady reconnaissance, enables VOLTZITE to avoid detection for lengthy periods of time.

Key Findings

- Targeting the electric sector, satellite, telecommunications, emergency management, and defense industrial bases.
- Targeting networks in the United States and Africa.
- Conducts slow and steady reconnaissance against a target.
- Employs mostly living off the land (LOTL) techniques and exhibits a high level of operational security practices.
- Deploys various web shells and FRP, a fast reverse proxy tool, for command and control (C2) communications
- C2 traffic frequently talks back to compromised SOHO (Small Office and Home Office) networking equipment or adversary leased VPS (Virtual Private Server) infrastructure.
- Uses open-source tooling and web shells.
- Leverages credential theft to facilitate lateral movement.
- Overlaps with multiple threat groups: Volt Typhoon (Microsoft), BRONZE SILHOUETTE (Secureworks), Vanguard Panda (Crowdstrike), and UNC3236 (Mandiant).

Overview of VOLTZITE

VOLTZITE is a threat group that targets the electric sector and other industrial sectors in the United States and other parts of the world. VOLTZITE conducts offensive operations with a significant focus on detection evasion and sophisticated operational security tradecraft. VOLTZITE frequently utilizes living off the land (LOTL) techniques and often tunnels command and control traffic through compromised SOHO routers. VOLTZITE's assessed intent is data exfiltration and long-term espionage.

VOLTZITE has overlaps with Volt Typhoon (Microsoft), BRONZE SILHOUETTE (Secureworks), Vanguard Panda (Crowdstrike), and UNC3236 (Mandiant).

These groups have tracked activity clusters dating as far back as 2021. Dragos makes the assessment of overlap to these groups based on the premise of strong correlating evidence on the victimology, infrastructure, and capabilities vertices of the Diamond Model of Intrusion Analysis.

Activity Timeline

Dragos has observed VOLTZITE since early 2023, but they are assessed with low confidence to have been active as far back as 2021, and have potential overlaps with KOSTOVITE, another Dragos-tracked threat group. The following provides a high-level timeline of VOLTZITE-related incidents tracked by Dragos.

2023

EARLY
- US Territory of Guam compromise.

JUN
- **VOLTZITE** infiltrates United States emergency management organization.

JUL
- Dragos discovers **VOLTZITE** targeting African electric transmission and distribution providers.

NOV
- Dragos collaborated with E-ISAC on analysis of **VOLTZITE** activity against multiple US-based electric sector organizations.

DEC
- Dragos discovered evidence that **VOLTZITE** has overlaps with UTA0178, a threat activity cluster tracked by Volexity, exploiting Ivanti ICS VPN zero-day vulnerabilities.

2024

JAN
- Extensive reconnaissance of a US telecommunication's providers external network gateways.
- Evidence of compromise against a large US city's emergency services GIS network.

Investigating VOLTZITE Compromise of a US Water & Electric Utility

In the early part of 2023, the VOLTZITE threat group compromised a U.S. water and electric utility and exfiltrated sensitive information. This data encompassed details on operational processes, configurations of operational technology (OT) assets, geographic information system (GIS) data, SCADA system configurations, and lists of critical customers.

The utility took steps to bolster its cybersecurity posture in late 2023. It implemented the Dragos Platform to monitor and secure IT-OT network traffic at Purdue Model Levels 3-4 and OT-OT communications at Level 2. Additionally, the utility engaged OT Watch, a team of industrial threat hunters at Dragos, to identify and neutralize persistent threats.

OT Watch confirmed VOLTZITE's actions were in close proximity to the utility's OT. Specifically, the Dragos Platform identified server message block (SMB) traversal maneuvers, and remote desktop protocol (RDP) lateral movement, illustrating VOLTZITE's strategy to navigate and pivot within the network to access OT data. The investigation found that VOLTZITE was focused on accessing and exfiltrating sensitive documents and data that are pivotal to critical operations of the electric utility.

Dragos Intelligence assesses with moderate confidence that the initial compromise, rapid data exfiltration, and proximity to the OT network, followed by VOLTZITE's return to the network months later, highlights an intent to maintain long-term persistence in networks of interest for follow-on actions in the future.

The employment of living off the land (LOTL) techniques and credential reuse by VOLTZITE, along with slow and steady reconnaissance, enables the group to avoid detection. VOLTZITE activity is unlikely to be picked up by traditional detection methods. This strategy allows VOLZITE to stretch out their dwell time within a network. Dragos recommends monitoring cross-zone communications between IT and OT networks and utilizing behavioral detections engineered to identify the latest VOLTZITE tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs).

In response to these events, Dragos OT Watch launched subsequent hunts across the fleet of subscribed customers, and Dragos Intelligence analyzed Neighborhood Keeper participant data for indications of VOLTZITE behaviors and anonymously alerted impacted parties. Additional behavioral detections were developed based on new TTPs identified during the investigation and were deployed to the Dragos Platform to ensure detection capabilities across the customer base.

Capabilities

VOLTZITE compromises external network perimeter applications and assets such as SOHO routers and virtual private network gateways to gain access to targeted organization's networks. Once within the victim's network, they leverage LOTL techniques and stolen credentials to move through the network.

Examples of exploited applications:

- Fortinet FortiGate
- PRTG Network Monitor appliances
- ManageEngine ADSelfService Plus
- FatPipe WARP
- Ivanti Connect Secure VPN
- Cisco ASA

Lateral Movement Tactics, Techniques, and Procedures

VOLTZITE has exhibited differing techniques for credential access and lateral movement once inside a network. The first observed technique is the use of csvde.exe, which is a native Windows binary used for importing and exporting data from Active Directory Domain Services using the comma-separated values (csv) file format. Obfuscation techniques are also employed.

The second observed technique to steal credentials for lateral movement is using Volume Shadow Copies and the extraction of the NTDS.dit Active Directory database from a domain controller. Volume Shadow Copies are cloned images of the operating system that can be used as backups or restoration points for an administrator to roll back a Windows machine if any issues arise with the operating system later. The NTDS.dit database, which is stored on domain controllers, is effectively the database underpinning all the information in Active Directory about user accounts, groups, computers, and most importantly, the hashes of user passwords. Under normal circumstances, the NTDS.dit file cannot be opened or copied as it is in use by Active Directory on the machine. To circumvent this protection, adversaries commonly use the Volume Shadow Copy Service to create a cloned image of the operating system and save it to a disk. Then the adversary can exfiltrate the copy of NTDS.dit residing in the shadow copy with no issues, as that file version is not in use by any processes. Once the NTDS.dit database is back on an adversary's machine, they can perform hash cracking or come back to the victim machine and use "pass the hash" techniques to authenticate as a user.

Infrastructure

VOLTZITE uses very minimal tooling and prefers to conduct their operations with as little a footprint as possible, hence their favoritism for LOTL techniques. However, VOLTZITE has been observed using the FRP reverse proxy tool and multiple web shells.

FRP is a proxy that allows you to expose a machine behind a firewall or network that maps multiple private IP addresses to a public address through Network Address Translation (NAT). FRP can be used to channel data directly to a command-and-control server and not follow the usual egress points out of a network.

VOLTZITE has compiled FRP binaries and utilized them as a command-and-control mechanism through some of their attacks. VOLTZITE has primarily utilized web shells based off the Awen web shell. VOLTZITE web shells result in primarily LOTL techniques to be used as follow-up actions. Once VOLTZITE infiltrates a network via an initial access point and then deploys a web shell, the most common subsequent action is the adversary familiarizing themselves with the environment they are in by running Windows native tools such as 'whoami' or 'tasklist'.

VOLTZITE has also exhibited heavy use of LOTL techniques. The Windows tools that VOLTZITE uses include but are not limited to the following:

- Certutil
- dnscmd
- Ldifde
- Makecab
- net user/group/use
- netsh
- nltest
- ntdsutil
- PowerShell
- reg query/save
- systeminfo
- tasklist
- wevtutil
- wmic
- xcopy

Impact to Industrial Control Systems (ICS)

To date, Dragos has only observed VOLTZITE operations achieving Stage 1 of the ICS Cyber Kill Chain. They have not yet displayed actions or capabilities designed to disrupt, degrade, or destroy ICS/OT assets or operations. However, their persistent targeting of critical infrastructure entities and observed capabilities could result in aiding the development of an ICS-capable disruption tool.

VOLTZITE has shown continued interest in the electric and telecommunications sectors in the United States. This is evidenced by long-term slow and steady reconnaissance and enumeration of multiple electric entities. If VOLTZITE can establish an initial foothold on the network perimeter of a target, they may then be able to pivot further into a victim's information technology (IT) network. Once access is established, VOLTZITE conducts espionage activities via LOTL techniques to attempt detection evasion. If proper network segmentation between the IT and operational technology (OT) networks of a victim is not apparent, then VOLTZITE may laterally move into OT networks to perform enumeration and data exfiltration of critical OT operational data such as SCADA data, OT device configurations, historian data, Geographic Information Systems (GIS) data, amongst others.

Recommendations

Considering the risk and related threats, Dragos recommends organizations implement the 5 Critical Controls for World-Class OT Cybersecurity identified by the SANS Institute - which presents a framework for implementing a cybersecurity program to defend against adversary activity directed against OT networks, be it IP (Intellectual Property) theft, ransomware, or targeted cyber-physical effects.

A first step in implementing these controls is achieving executive alignment on the role and importance of OT cybersecurity and the specific risks an OT cybersecurity program is meant to defend against, if not well understood. One potential way to achieve organizational alignment is to tie the effort back to real-world scenarios. The information detailed above clearly outlines the capabilities developed for the adversary and their intended impacts. This detail can

be instrumental in understanding how the capabilities might impact a given network, the potential operational and business implications, and the steps necessary to defend against and remediate the potential effects.

Translating cyber risks into the impact on an organization's operations and functions can help executive stakeholders engage on the topic of OT cybersecurity. Once an organization can achieve executive and board-level alignment on the importance of investing in OT cybersecurity, the foundation is in place for the implementation of the five critical controls for OT cybersecurity which are shown below:

1. ICS Incident Response
Operations-informed incident response (IR) plan with focused system integrity and recovery capabilities during an attack—exercises designed to reinforce risk scenarios and use cases tailored to the ICS environment.

2. Defensible Architecture
Architectures that support visibility, log collection, asset identification, segmentation, industrial DMZs (Demilitarized Zones), and process-communication enforcement.

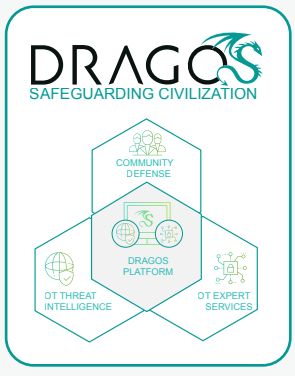
3. ICS NETWORK VISIBILITY MONITORING
Continuous network security monitoring of the ICS environment with protocol-aware toolsets and system of systems interaction analysis capabilities used to inform operations of potential risks to control.

4. SECURE REMOTE ACCESS
Identification and inventory of all remote access points and allowed destination environments, on-demand access, and multi-factor authentication (MFA), where possible, jump host environments to provide control and monitor points within the secure segment.

5. RISK-BASED VULNERABILITY MANAGEMENT
Understanding the cyber digital controls in place and device operating conditions that aid in risk-based vulnerability management decisions to patch for the vulnerability, mitigate the impact or monitor for possible exploitation

Conclusion

VOLTZITE poses a credible threat to critical infrastructure operators in the United States and jurisdictions within the threat group's strategic interest. VOLTZITE heavily focuses on detection evasion and long-term persistent access with the assessed intent of long-term espionage and data exfiltration. Dragos recommends that industrial organizations familiarize themselves with all potential detection mechanisms for LOTL techniques, with a focus on anomaly and behavior-driven threat detection strategies.



About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Learn more about our technology, services, and threat intelligence offerings:

Request a Demo | Contact Us