Threats Groups Targeting the Energy Sector

Voltzite

Emily Eubanks | malwaremily

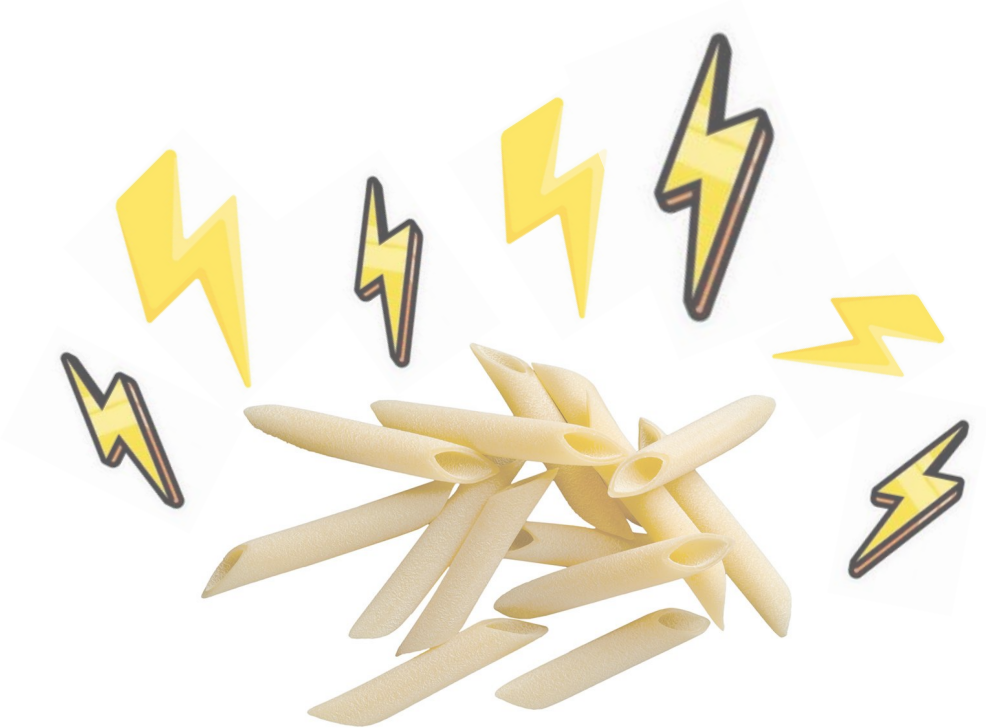
VOLTZITE - Targets

NATIONS

- United States of America
- Non-continental U.S. Territories (i.e. Guam)
- UK
- Australia

INDUSTRIES

- Energy
- Telecommunication
- Transportation Systems
- Water and Wastewater Systems
- Satellite Services
- Emergency Management Services



VOLTZITE - Targets

NATIONS

- United States of America
- Non-continental U.S. Territories (i.e. Guam)
- UK
- Australia

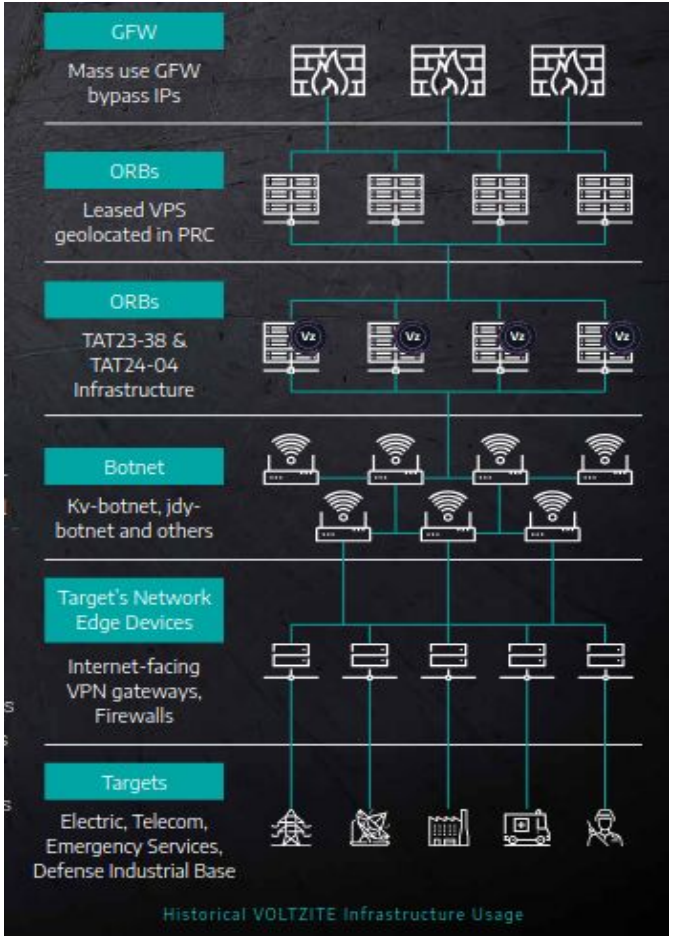
INDUSTRIES

- Energy
- Telecommunication
- Transportation Systems
- Water and Wastewater Systems
- Satellite Services
- Emergency Management Services

VOLTZITE - Infrastructure

CHARACTERISTICS

- Named by Dragos (2023)
- Extensive technical overlap with…
  - Volt Typhoon
  - UTA0178
- Focus on stealing OT related data
  - network diagrams
  - OT equipment diagrams, documents
  - Data on SCADA systems, relays, switchgear
  - Graphical Information System (GIS) data
- GIS data examples: siting new locations for solar, wind, geothermal generation, mapping transmission lines, etc.
- Operational Relay Box (ORB) networks
- Shares PRC affiliated threat actor infrastructure



VOLTZITE - Behaviors

PRECOMPROMISE

- ORB network, compromised SOHO/VPS systems (kv-botnet, jdy-botnet)
- Multi-hop proxies
- enumerate internet-exposed servers

INITIAL ACCESS

- Exploit known or zero-day vulnerabilities in public-facing network appliances
  - Fortinet
  - Ivanti (formerly PulseSecure)
  - NETGEAR
  - Citrix
  - Cisco
  - PRTG Network Monitor

VOLTZITE - Behaviors

POSTCOMPROMISE

- Slow, steady, extensive reconnaissance to identify…
  - network topologies
  - security measures
  - typical user behaviors
  - key network and IT staff
- Long-term persistence (i.e. 5+ years) with dedicated resources to maintain persistence and understand the target environment over time.
- Valid Accounts
- LOTL techniques (TTPs tailored to victim environment)

VOLTZITE - Behaviors (POSTCOMPROMISE cont'd)

DISCOVERY

- cmd
- certutil
- dnscmd
- ldifde
- makecab
- net user/group/use
- netsh
- nltest
- netstat
- ntdsutil
- ping
- PowerShell
- quser
- reg query/reg save
- systeminfo
- tasklist
- wevtutil
- whoami
- wmic
- xcopy

- **`net start` used to list running services**

VOLTZITE - Behaviors (**POSTCOMPROMISE cont'd**)

DEFENSE EVASION

- PowerShell used to query WEL; extraction Security logs via .dat files
- Targeted log deleted to evade detection (WEL, system).
- Masquerade binaries (e.g. rar.exe → ronf.exe)

CREDENTIAL ACCESS

- vssadmin to create shadow copy (cracks passwords offline)
- ntdsutil to copy NTDS.dit and SYSTEM hive from volume shadow copy
- Outdated comsvcs.dll downloaded to non-standard folder, LSASS dumped with MiniDump
- Interacted with PuTTY application to enumerate stored sessions
- Interact with browser artifacts to obtain stored passwords

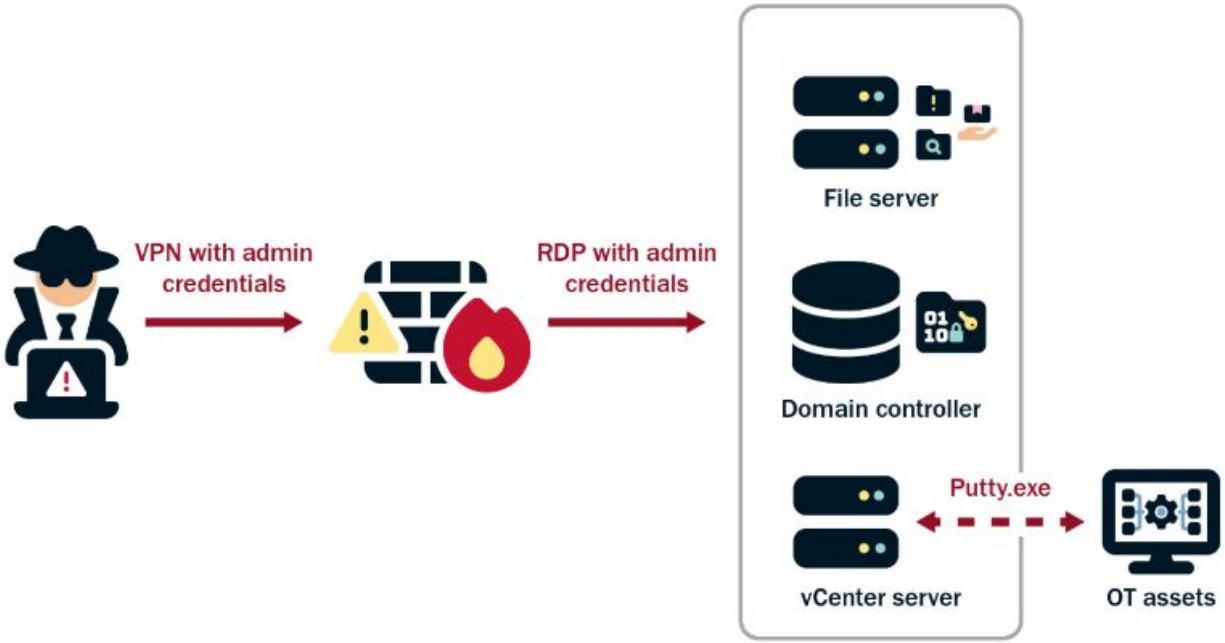


Figure 2: Volt Typhoon Lateral Movement Path File Server, DC, and OT-Adjacent Assets

Source: CISA Joint Cybersecurity Advisory [1]

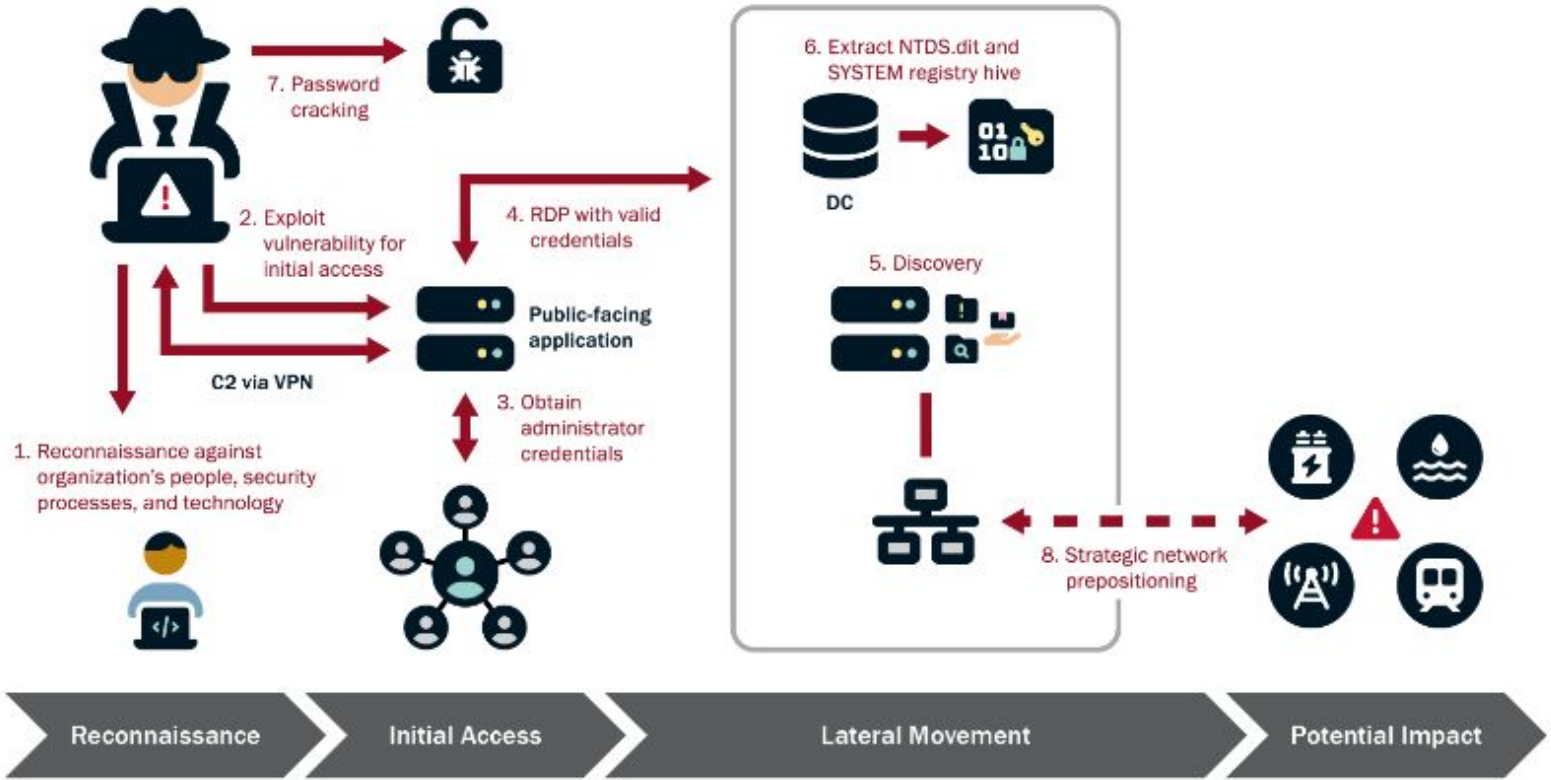
VOLTZITE - Behaviors (**POSTCOMPROMISE cont'd**)

COLLECTION & EXFILTRATION

- WMIC used to create and use temporary directories
- Renamed Winrar to compress exfil data
- Exfiltration via SMB

NONNATIVE TOOLS

- Magnet RAM Capture (MRC)
- Fast Reverse Proxy (FRP) (obfuscated client files with UPX)
- Mimikatz
- Impacket
- Existing tools found on victim endpoints (e.g. Advanced IP Scanner)



Source: CISA Joint Cybersecurity Advisory [1]

VOLTZITE - Examples

Voltizite threat actors have been observed…

- Abstaining from using compromised credentials outside of normal working accounts
- Obtaining credentials insecurely stored on public-facing network appliances
- Testing access to domain-joint OT assets using OT vendor credentials, or leverage credentials cracked in NTDS.dit dump from shadow copy
- After successful lateral movement to OT environment, minimal activity is observed beyond occasional discovery activity.
- Extremely long dwell time, Dragos reports evidence of Voltzite extracting NTDS.dit from three DCs within a four year period in one compromise, another victim they extracted twice within a 9 month period.
- Storing data in .log file detailing user activities, user PowerShell commands, keypresses, internet browsing activity; includes Timestamps.

VOLTZITE - Objective Theories

- “*Volt Typhoon actors are pre-positioning themselves on IT networks to enable lateral movement to OT assets to disrupt functions.*” Source: CISA
- Craft malicious OT-specific tooling to disrupt critical systems (Dragos)
- Positioning to act in the event of geopolitical escalation and/or military conflict.
-

VOLTZITE - Objective Theories

Robert M. Lee (Dragos) discusses a 300+ day intrusion:

“***It was very clear that the adversary, though contained to the enterprise IT network, was explicitly trying to get into the OT network there [...] I can confirm that they were stealing a lot of OT-specific data and insights, and SCADA-related information and GIS-related information, and things that would be useful in future disruptive attacks [...] It was clear that Voltzite was specifically thinking about key targets and how to take down power in the future, based on what they were stealing.***”

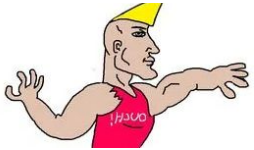
Source: Dark Reading [4]

VOLTZITE - US FEDERAL RESPONSE ACTION

- FBI announced it shut down a botnet of compromised network devices associated with PRC ORB network. [5]
- "*A December 2023 court-authorized operation has disrupted a botnet of hundreds of U.S.-based small office/home office (SOHO) routers hijacked by People's Republic of China (PRC) state-sponsored hackers [...]*
- *privately-owned SOHO routers infected with the "KV Botnet" malware to conceal the PRC origin of further hacking activities [...]*
- *[...] the government extensively tested the operation on the relevant Cisco and NetGear routers. The operation did not impact the legitimate functions of, or collect content information from, hacked routers. Additionally, the court-authorized steps to disconnect the routers from the KV Botnet and prevent reinfection are temporary in nature. A router's owner can reverse these mitigation steps by restarting the router. However, a restart that is not accompanied by mitigation steps similar to those the court order authorized will make the router vulnerable to reinfection.*
- *The FBI is providing notice of the court-authorized operation to all owners or operators of SOHO routers that were infected with the KV Botnet malware and remotely accessed pursuant to the operation. For those victims whose contact information was not publicly available, the FBI has contacted providers (such as a victim's internet service provider) and has asked those providers to provide notice to the victims.*"

VOLTZITE - THaDE

- Meticulous network monitoring for unusual communication
- Subset of common discovery commands with administrative overlap



- LOTL anomalies that deviate from baseline
- Windows ESENT Application logs for evidence of NTDS.dit copy. (ESENT App ID 216,325,326,327)
- vssadmin creating shadow copy
- download DLL (comsvcs.dll) to non-standard folder
- PowerShell queries against WEL saved to **.dat** file
- WEL deletion via EID 1102
- Native executables in non-standard folders

- [?] Extract SYSTEM Registry Hive
- [?] PTH Techniques
- [?] FRP Reverse Proxy Tool
- [?] csvde utility execution

VOLTZITE - MITIGATIONS

- MFA, least priv, gMSAs & PAM+RBAC
- Don’t leave your passwords laying around
- Don’t let your users leave their passwords laying around
  - Configure group policy settings to prevent web browsers from saving passwords and disable autofill functions.
- Regularly roll NTLM hashes of accounts that support token-based auth
- Securely store sensitive data (like OT documentation)
- Establish and continuously maintain a baseline of installed tools and software, account behavior, network traffic.
- Audit security, access, application logging to ensure it aligns with expectation
- Validate security controls

References

[1] Joint Cybersecurity Advisory ‘PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure’. Published 2024 Feb 07. https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf

[2] Dragos. 2025 OT/ICS Cybersecurity Report | Year in Review. Published 2025. https://hub.dragos.com/hubfs/312-Year-in-Review/2025/Dragos-2025-OT-Cybersecurity-Report-A-Year-in-Review.pdf?hsLang=en

[3] Mandiant (Michael Raggi). IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders. Published 2024 MAY 22. https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks

[4] Dark Reading. Web article. Published. https://www.darkreading.com/vulnerabilities-threats/volt-typhoon-hits-multiple-electric-cos-expands-cyber-activity

[5] U.S. Department of Justice. Press Release ‘U.S. Government Disrupts Botnet People’s Republic of China Used to Conceal Hacking of Critical Infrastructure’. Published 2024 JAN 31. https://www.justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical