2026 Electric OT

Threat Trends and Defensive Priorities

Phil Tonkin

Field CTO - Electricity

DRAGOS

9th Annual Dragos Year in Review

New specialized threat groups with diverse approaches lower the barrier for established groups to achieve OT impact

Control loop mapping demonstrates **adversaries understand industrial operations at the process level**

Shift from reconnaissance to **attempted operational effects throughout 2025**

Ransomware incidents are OT by consequence despite frequent oversimplification and mislabeling

Organizations still struggle to implement basic controls, preventing an effective response when attacks occur

Dragos Identifies 3 New Threat Groups

Of the 26 threat groups tracked by Dragos, 11 were active in 2025

New: SYLVANITE

Rapid exploitation broker enabling VOLTZITE access to critical infrastructure

SINCE 2025

Sy

- Exploited Ivanti VPN vulnerabilities within 48 hours of disclosure
- Extracted Active Directory credentials
- Installed persistent web shells on F5 devices
- Handed off access to VOLTZITE or deeper intrusions

Targets:

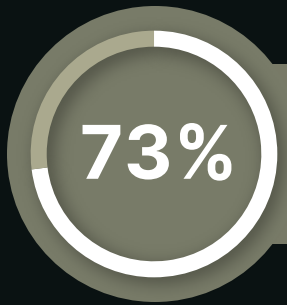

Electric Power


Water


Oil & Gas


Manufacturing


Public Administration



of Dragos IR cases involved active exploitation or credential reuse of VPN/jumphosts

Overlaps with: UNC5221, UNC5174, UNC5291, UNC3236, HOUKEN, Red Dev 61, CL-STA-0048, UTA0178

Rapid Vulnerability Exploitation Campaigns

Dec 2023 — 1

Ivanti Connect Secure CVE-2023-46805, CVE-2024-21887

2024 — 2

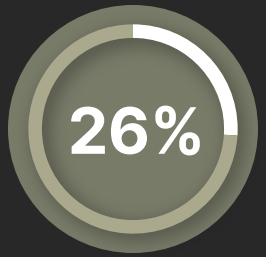
F5 BIG-IP & ConnectWise ScreenConnect; F5: CVE-2023-46747; ConnectWise: CVE-2024-1709

Apr 2025 — 3

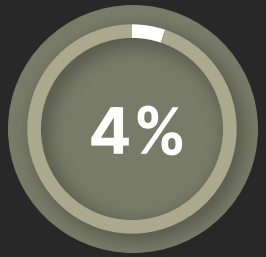
SAP NetWeaver Zero-Day CVE-2025-31324

May 2025 — 4

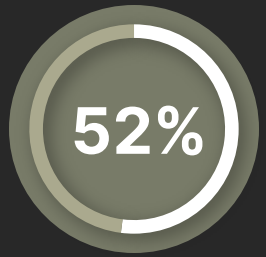
Ivanti EPMM (U.S. Utility Victim) CVE-2025-4427, CVE-2025-4428



of advisories had NO patch when announced



had public POC & were actively exploited



Dragos provided alternate mitigations when vendors couldn't

VOLTZITE

Demonstrated capability to access
& manipulate OT/ICS assets

- Exploited VPN gateways to access utility networks
- Extracted SCADA configuration files from engineering workstations
- Observed operational data to understand process shutdown conditions
- Maintained access through web shells on internet-facing appliances

Overlaps with: VOLT TYPHOON, BRONZE SILHOUETTE, VANGUARD PANDA, INSIDIOUS TAURUS

VOLTZITE Attack Path

01 Network perimeter reconnaissance

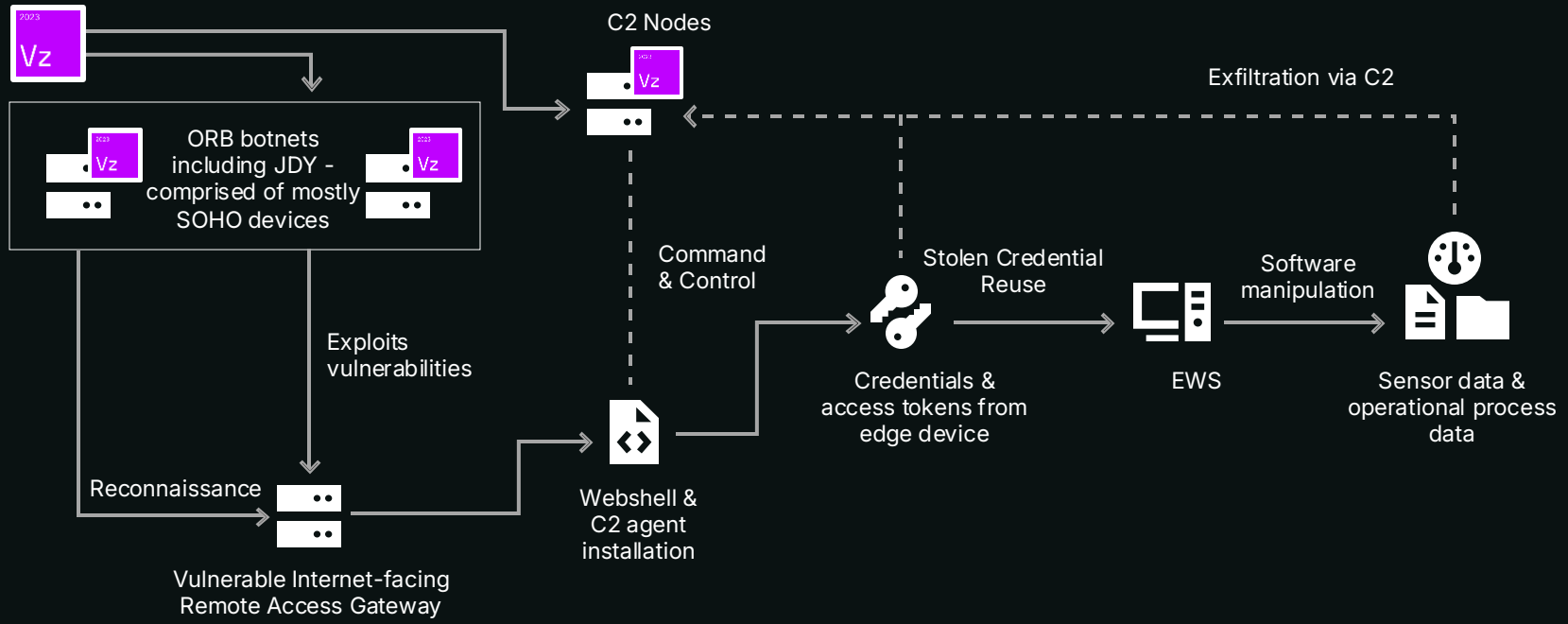
02 Compromise Internet-facing edge devices

03 Establish edge device persistence

04 Exfiltrate credential data from internet-facing edge devices

05 Replay legitimate credentials for lateral movement

06 Exfiltrate OT sensor and operational process data



New: AZURITE

Theft of operational information, long-term access enablement

SINCE 2021

Az

What Dragos Observed in 2025

- Compromised SOHO routers to build proxy infrastructure across multiple countries
- Exfiltrated OT network diagrams and operational data
- Accessed engineer workstations through compromised edge devices
- Maintained persistent access for extended periods using living off the land techniques

Targets:

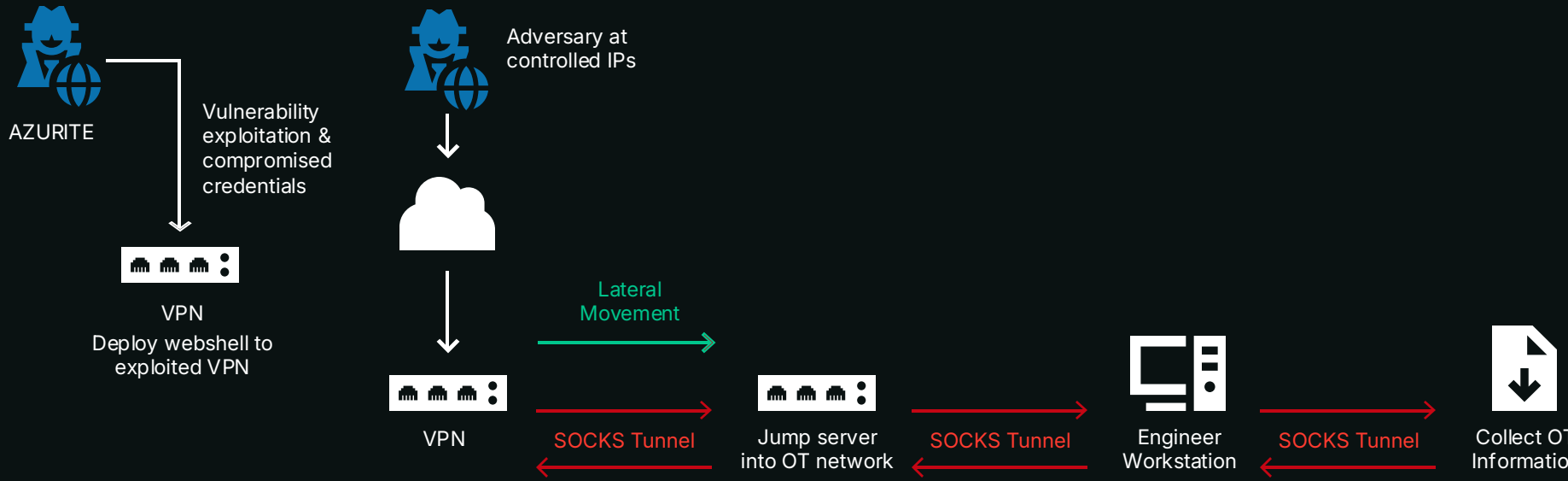
Manufacturing | Defense | Automotive | Electric | Government | Oil & Gas

Overlaps with: Flax Typhoon, Ethereal Panda, UNC5923, Raptor Train, Red Dev 54

AZURITE

VPN Access to OT Environment and Engineer Workstation

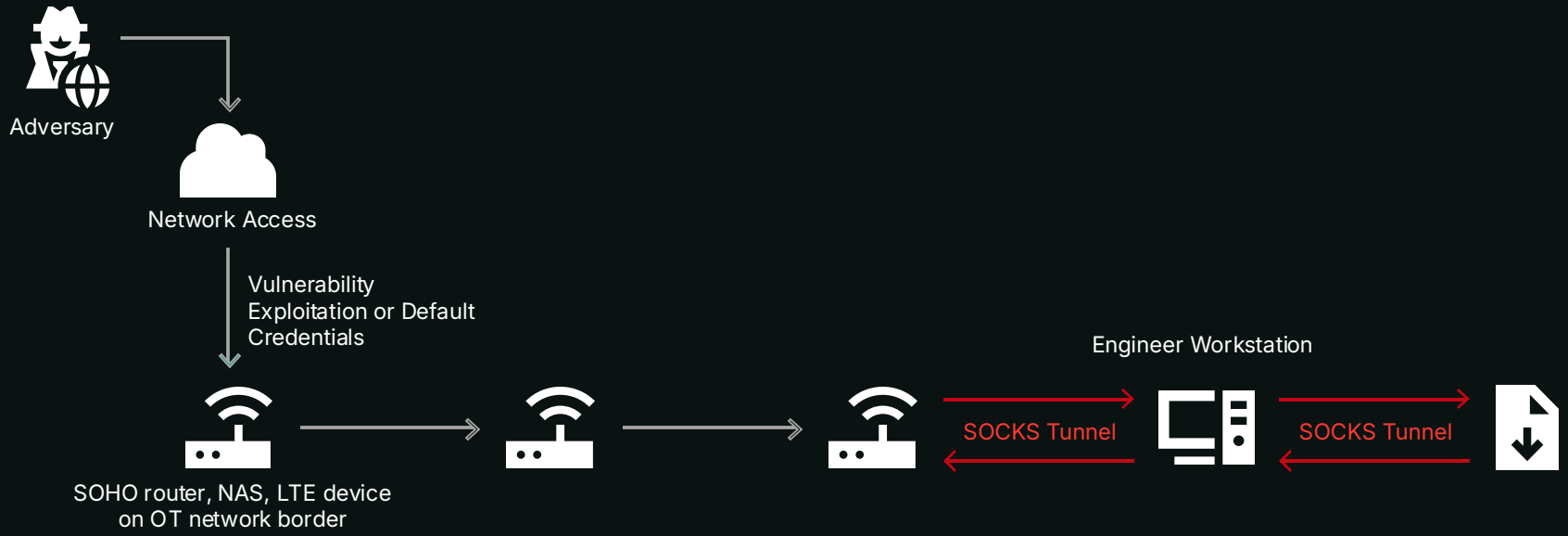
01	02	03	04	05
Exploit vulnerabilities or use VPN credentials from other credential stuffing	Deploy webshell to VPN device	Access OT jump server with compromised credentials	Access engineer workstation to exfiltrate OT operational information	Exfiltrate alarm data, PLC configurations, HMI data, operational information via SOCKS tunnels



AZURITE

SOHO Device Compromise to Achieve OT Access

01	02	03	04	05
Direct access to exposed SOHO devices	Enroll device into ORB network and/or stage capabilities on ORB	Pivot into OT network segment connection with the edge device	Identify and then access engineering workstations	Exfiltrate alarm data, PLC configurations, HMI data, operational information via SOCKS tunnels



New: PYROXENE

Cross-domain access enabling movement from IT into OT networks

SINCE 2025

Py

What Dragos Observed in 2025

- Created fake LinkedIn profiles posing as aerospace recruiters
- Used stolen credentials to access Citrix and VMware systems
- Compromised defense contractor websites to target employees
- Moved from corporate IT into operational technology networks

Targets:

Transportation | Logistics | Aerospace | Aviation | Utilities | Manufacturing

Overlaps with: APT35, Tortoiseshell, UNC1549, Imperial Kitten, assessed by the U.S. Government to be aligned with the Islamic Revolutionary Guard Corps Cyber Electronic Command (IRGC-CEC)

PYROXENE Attack Path

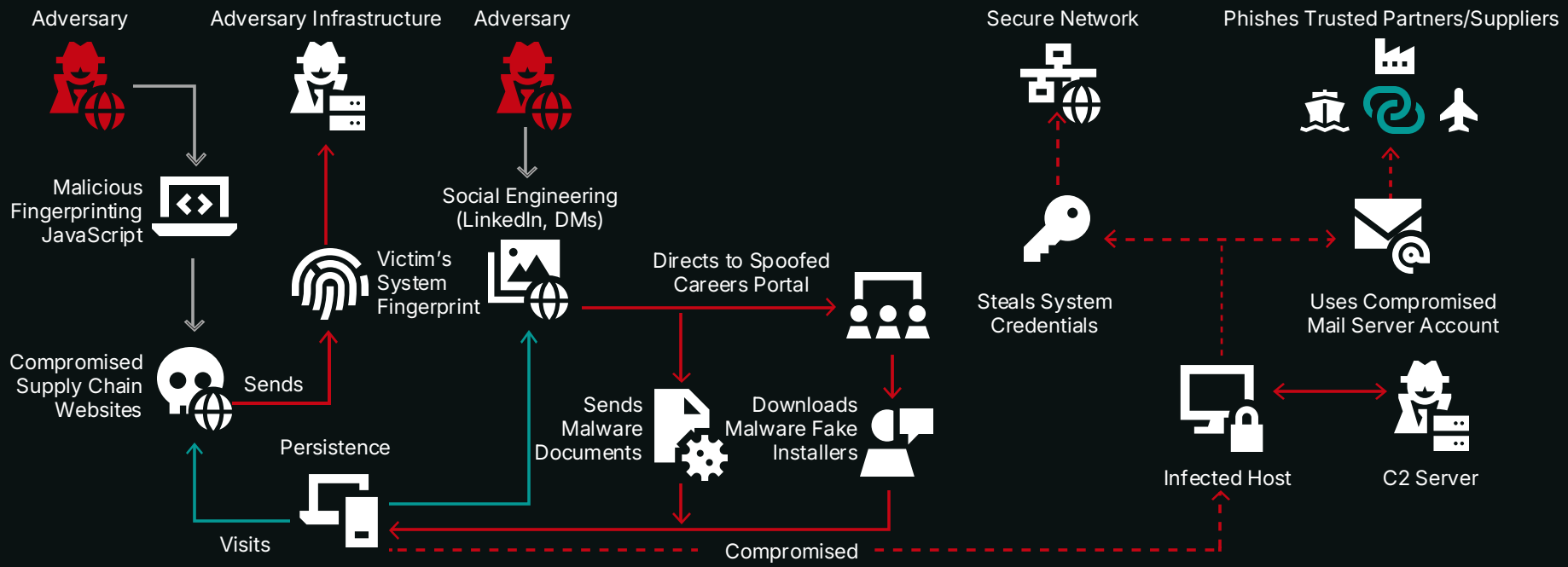
01 Strategic website compromises

02 Social engineering campaign

03 Deploy RAT/Backdoor Infect Victim Host

04 Lateral movement into secure network

05 Supply Chain Attack



Expansion of KAMACITE Targets

Targeted reconnaissance & access establishment enabling ELECTRUM attacks

- European supply chain campaign targeting 25+ Ukrainian ICS vendors and GIE conference attendees with multi-week social engineering
- U.S. reconnaissance scanning industrial devices:
  Schneider Altivar VFDs, Smart HMIs, Accuenergy AXM modules, Sierra Wireless AirLink gateways
- Industry-specific phishing using native languages and technical terminology
- Hands off established access to ELECTRUM for destructive Stage 2 operations

Systematic Targeting of Operational Workflows

KAMACITE U.S. Campaign (March-July 2025)

Targeted

- HMIs (command origin)
- VFDs (physical control)
- Meters (process visibility)
- Gateways (remote access)

Also Observed:

VOLTZITE: Dumps configs to find process stop triggers

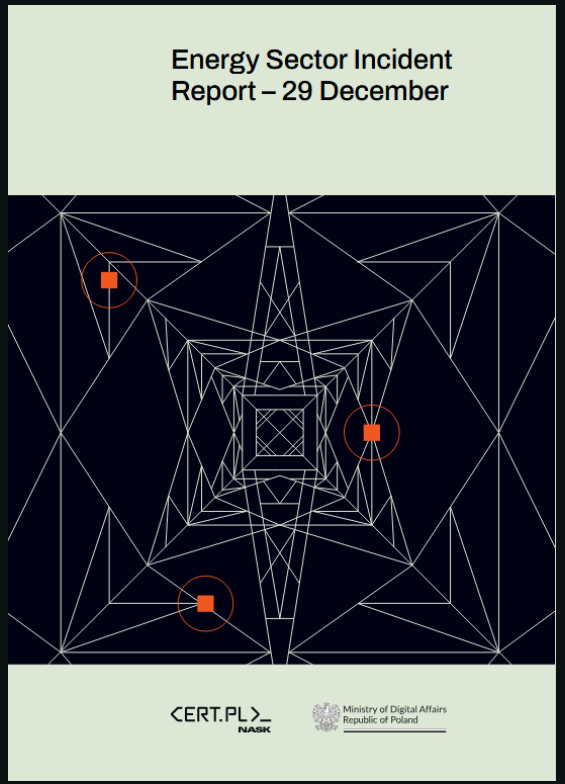
AZURITE: Exfiltrates alarm data for operational boundaries

Adversaries are mapping entire control loops for future targets & attacks.

Attack Targeting DER in Poland

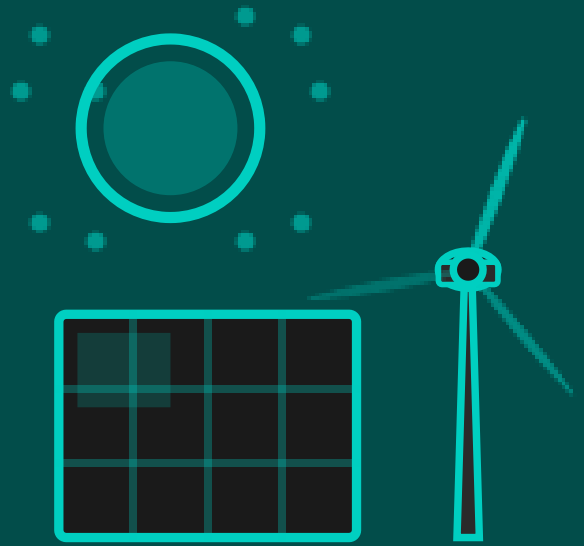
1st major attack targeting decentralized energy grids

- Combined Heat & Power (CHP) facilities + Renewable Energy Management Systems (wind/solar dispatch)
- Communications systems disabled at multiple sites
- No customer outages, but adversary had access to operational control systems
- Dragos attributes this attack with moderate confidence to ELECTRUM



A Warning for Renewable-Heavy Grids

The attack in Poland exposes vulnerabilities in tomorrow's grid



Poland's Grid Protected Them

- 50%+ thermal generation (coal/lignite) provided stabilizing inertia
- Only ~25% renewable capacity
- Strong AC interconnections with neighbors

Higher Renewable Penetration = Higher Risk

- Larger attack surface and lower system inertia
- Smaller facilities fall below bulk power regulations
- Each DER site has multiple remote access points

ELECTRUM: 10 Years of Practice

From manual breaker commands to automated grid attacks

December 2015

1

Coordinated attack on 3 Ukrainian distribution operators causing power outages during winter

December 2016

2

Deployed CRASHOVERRIDE malware against Ukrainian transmission substation affecting hundreds of thousands

2022-2025

3

Deployed Industroyer2, LOTL scripts targeting distribution automation, and multiple custom wipers

still can't detect Electrum-style attacks

ELECTRUM Playbook

Specialized capability to cause physical disruption of electrical grids & industrial processes

- PathWiper malware; destroys MBR, NTFS metadata, and all mounted volumes
- Coordinated destructive operation against 8 Ukrainian ISPs using Solntsepek hacktivist persona
- New destructive wiper variant, continuing toolkit evolution

BAUXITE

Direct ICS manipulation and destructive operations targeting internet-exposed operational technology

2023

Bx

What Dragos Observed in 2025

- Threatening email campaign targeting cybersecurity vendors, ICS researchers, and media
- Deployed two wiper malware variants against Israeli targets during Iran-Israel conflict
- Continued Stage 2 activity: Direct manipulation of internet-exposed HMIs, PLCs, and industrial devices

Targets:

Critical infrastructure globally, with focus on organizations with internet-exposed OT devices

Overlaps with: CyberAv3ngers (hacktivist persona)

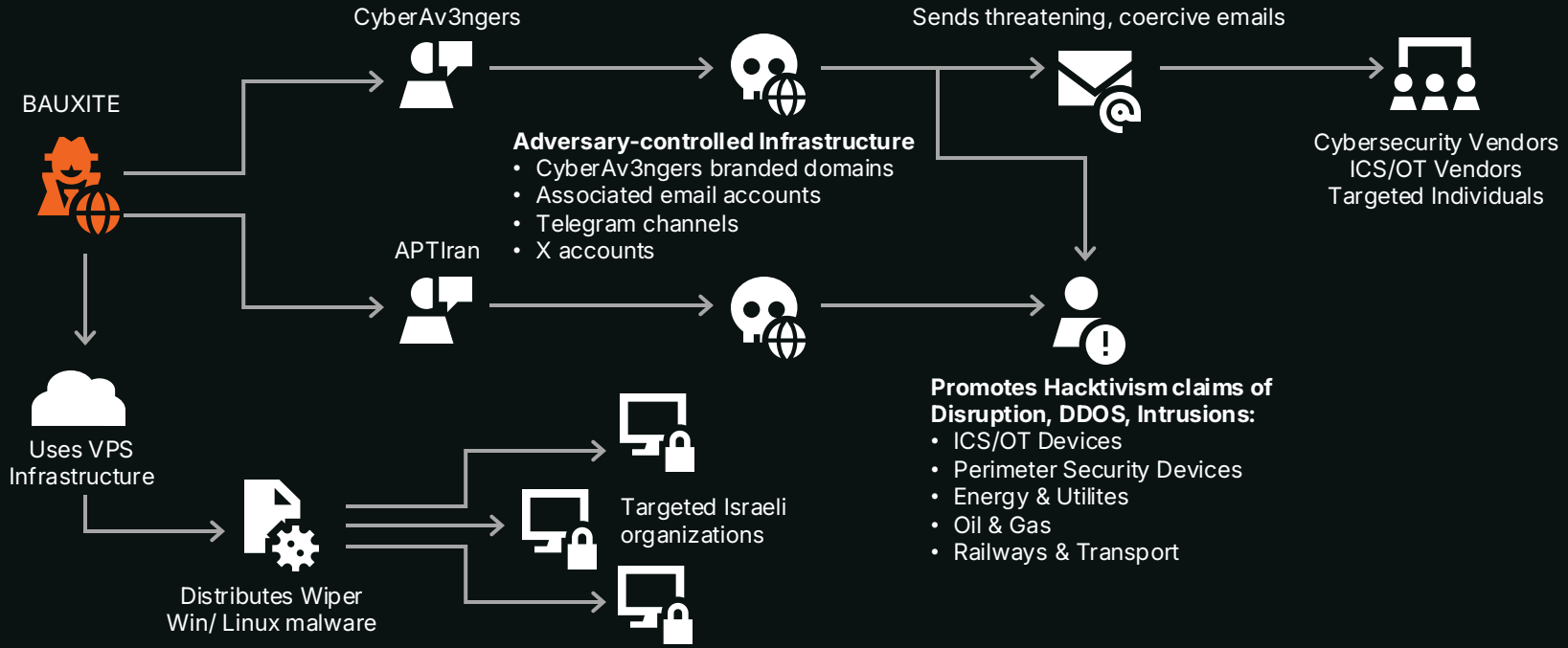
BAUXITE 2025 Activity

01

Psychological, Influence Operations

02

Destructive attacks against Israeli targets



Root Cause Analysis Problem

You can’t determine root cause if you lack monitoring BEFORE the incident.

30%

of IR cases began with “something is wrong”

82%

lack criteria for when operational anomalies trigger cyber investigation

Is it cyber?
Is it mechanical?
Is it operator error?

Many attacks don’t look like cyber

They’re just operational misuse of legitimate equipment

VOLTZITE config dumping looks like troubleshooting

KAMACITE VFD scanning looks like standard system enumeration

AI Compounds the Visibility Problem

Establish visibility BEFORE deploying AI or risk creating exponentially greater blind spots.

Organizations are deploying

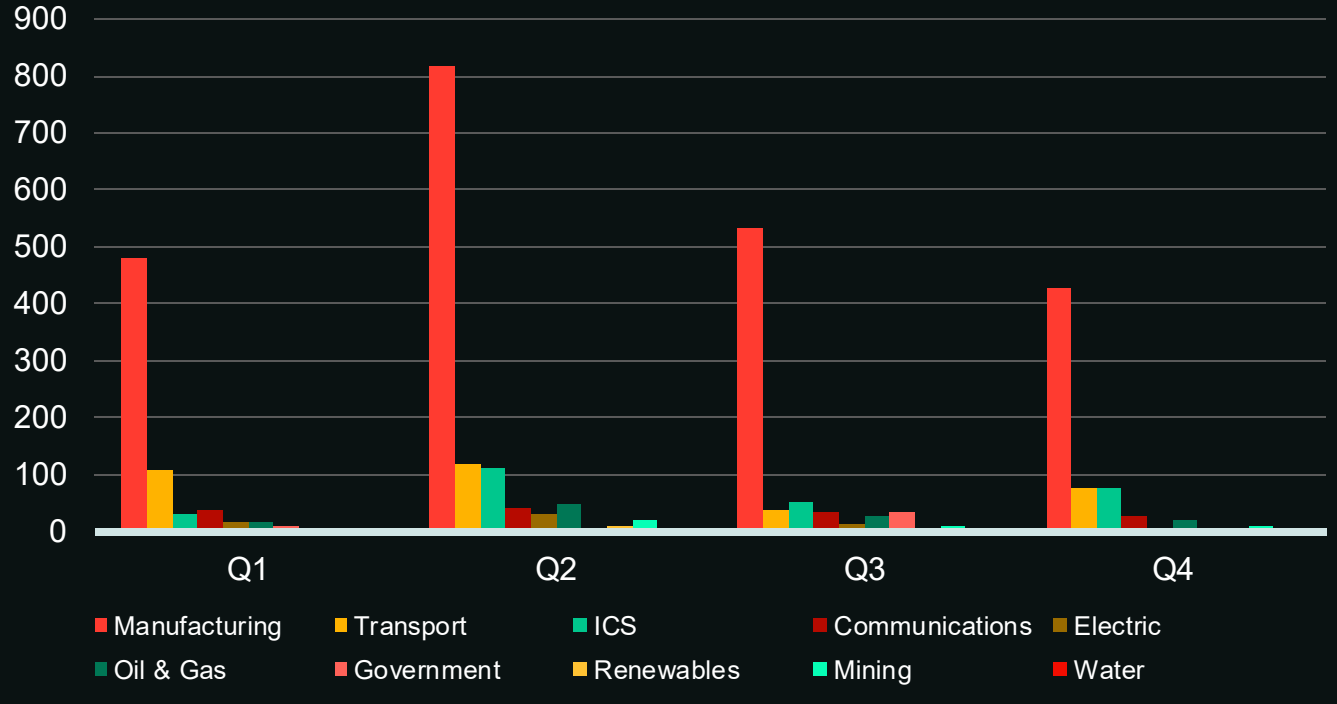
in operational environments without first establishing visibility.

> Was this cyber, equipment failure, AI error, or authorized change?

Impossible to answer without OT visibility & foundational telemetry already in place beforehand

Ransomware by Sector

In 2025, 3300 ransomware attacks targeted industrial organizations



5 days
average dwell time
(getting faster)

Ransomware in OT is Mislabeled as IT Problem

Don’t call it an IT breach if OT stops working

If you classify by operating system, you miss the operational impact.

If you classify by network segment, you miss IT/OT dependencies.

Classify by consequence:
Did operations stop? It's an OT incident.

> **“It only hit Windows systems.”**
>
> *Engineering workstations run Windows. HMIs run Windows. Historians run Windows.*

The State Of ICS/OT Vulnerabilities

15% of vulnerabilities Dragos assessed in 2025 had incorrect CVSS data

More Severe CVSS

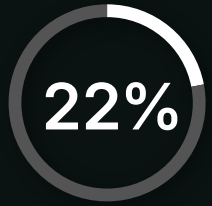
Less Severe CVSS

The Same

52% of advisories required Dragos to provide mitigations vendors didn't

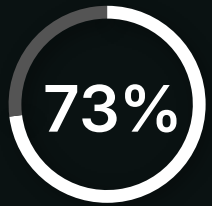
Where Vulnerabilities Reside

VULNERABLE ASSETS BORDERING THE ENTERPRISE ARE EXPLOITED FOR INITIAL ACCESS

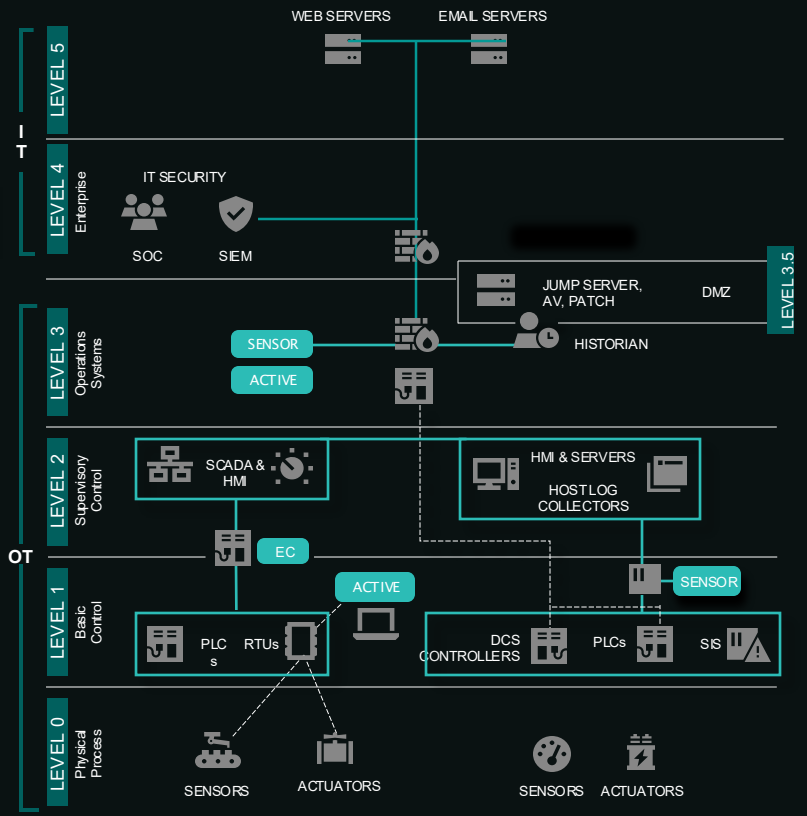


LEVELS
3.5 | 4 | 5

VULNERABLE ASSETS DEEP WITHIN ICS NETWORKS ARE CLOSE TO CRITICAL PROCESSES



LEVELS
0 | 1 | 2 | 3



Necessity of Risk-Based Decision

Only some vulnerabilities need immediate action

of ICS/OT vulnerabilities

needed to be addressed

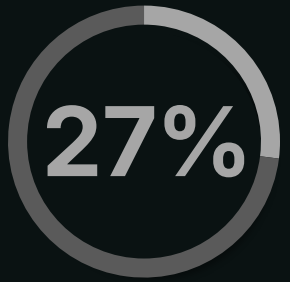
NOW

are network exploitable with no direct operational impact

These need to be addressed

NEXT

Mitigate through network monitoring, segmentation & MFA



pose a possible threat but rarely require action

They likely never need to be addressed

NEVER

Monitor these for signs of exploitation

Defenders Can’t Keep Up

Findings from pentests, tabletop exercises, assessments, and incident response

Can't **See** Fast Enough

have no OT visibility, impeding root cause analysis

detected ANY red team activity below IT/OT boundary

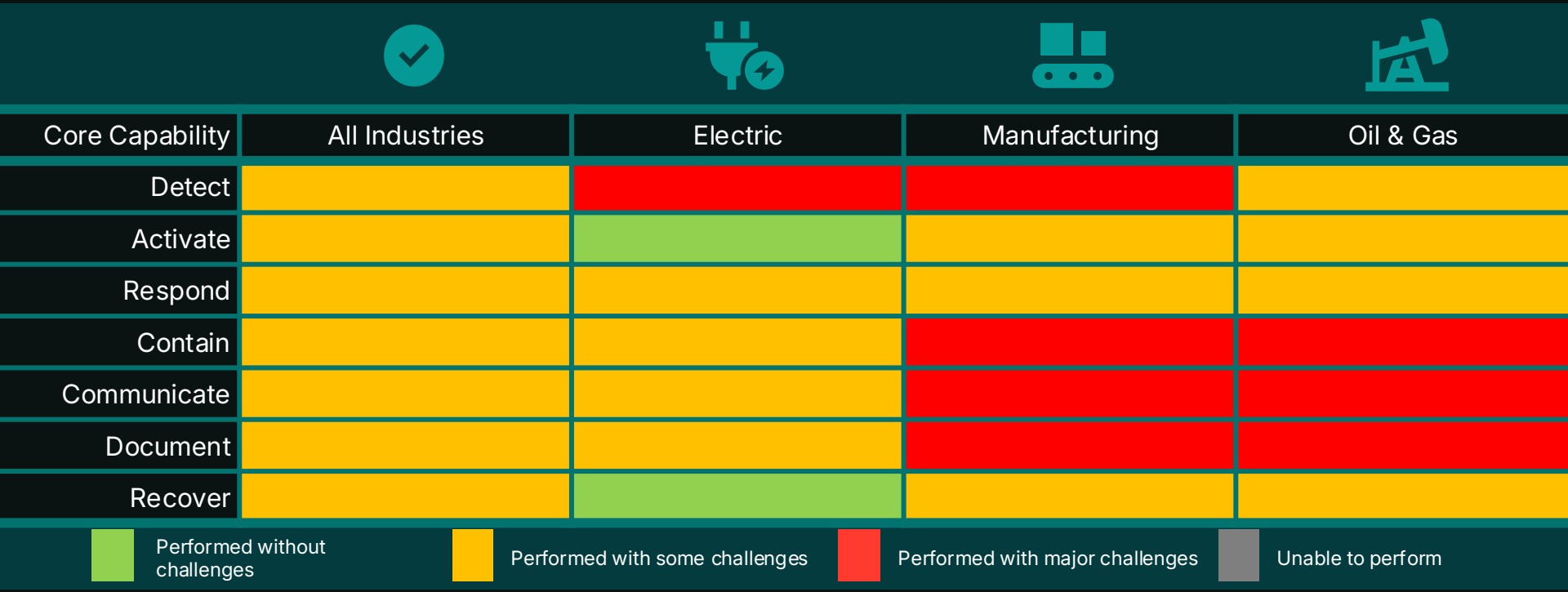
Can’t **Respond** Fast Enough

TTX struggled to detect & respond before process impact

recovery times

Are You Ready When It Matters?

Detection and containment remain the weakest capabilities across all sectors



Electric Sector Risks

Key threat themes converging on grid operations in 2025-2026

01 CONTROL-LOOP MAPPING

Adversaries are learning how your grid physically works

KAMACITE scanned U.S. HMIs, VFDs, meters, and cellular gateways in precise sequence for 4 months. VOLTZITE dumped alarm data from engineering workstations to understand what stops processes.

KAMACITE · VOLTZITE · AZURITE

02 DESTRUCTIVE CAPABILITY EXPANSION

ELECTRUM struck European DERs for the first time

December 2025: first coordinated cyberattack on distributed energy resources anywhere in the world. CHP plants and renewable energy management systems targeted in Poland. New PathWiper malware deployed. ELECTRUM's toolkit is actively growing, and KAMACITE is building access in the U.S.

ELECTRUM · PathWiper · DER Infrastructure

03 ACCESS-PROVIDER ECOSYSTEM

Breaches now happen in paired teams, faster than defenders adapt

SYLVANITE was caught inside a U.S. electric utility and handed access to VOLTZITE within days. These paired Stage 1/Stage 2 operations compress the timeline from initial compromise to OT-capable intrusion from weeks to days. The access developers and the attackers are different groups.

SYLVANITE → VOLTZITE handoff

OPERATIONAL CONSEQUENCES

Loss of View

Operators cannot trust sensor data or telemetry. ELECTRUM's attacks degrade confidence in what the grid is doing, not just whether it's running.

Loss of Control

Alarm and config data theft gives adversaries the blueprint to issue valid-looking commands. VOLTZITE specifically mapped what stops processes.

Physical Impact

ELECTRUM already caused power outages in 2015–16. Its DER attack in 2025 marks the first major assault on renewable infrastructure globally.

Active Threat Groups

Who is targeting electric – and how?

ELECTRUM

Stage 2

Crossed from Ukraine into Europe for first time

In December 2025, ELECTRUM struck Polish energy infrastructure — targeting combined heat and power (CHP) facilities and renewable energy management systems. This was the first major coordinated cyberattack against distributed energy resources (DERs) anywhere in the world. ELECTRUM is the most operationally experienced Adversary Dragos tracks.

- PathWiper destructive malware (new, June 2025)
- Solntsepek hacktivist persona used for attribution masking
- Paired with KAMACITE for persistent access

VOLTZITE

Stage 2

Upgraded to Stage 2 — now manipulating EWS

VOLTZITE compromised Sierra Wireless Airlink gateways at electric organizations and pivoted to engineering workstations, where it manipulated software to dump config files and alarm data — specifically to understand what would trigger operational processes to stop. This elevated VOLTZITE to Stage 2 status.

- Sierra Wireless Airlink RV50/RV55 exploitation
- GIS data exfiltration (Trimble Cityworks CVE-2025-0994)
- JDY botnet pre-staging VPN appliances

KAMACITE

Stage 1

Scanned U.S. control loops for 4 months straight

Mar–Jul 2025: KAMACITE conducted sustained internet reconnaissance of U.S.-exposed industrial devices — Schneider Altivar VFDs, Smart HMIs, Accuenergy AXM modules, Sierra Wireless Airlink gateways. Sequence implies intent to map entire control loops, not just identify devices. Feeds access to ELECTRUM.

- Targeted Schneider Altivar VFDs (CVE-2025-7746)
- Sierra Wireless Airlink gateway scanning
- Shifted to U.S. directly after retiring European campaign infra

SYLVANITE

Stage 1

Directly observed in U.S. electric utility in 2025

SYLVANITE was confirmed inside a U.S. electric utility during IR. It provides initial access to VOLTZITE within days of compromise. Exploits Ivanti EPMM, F5, SAP NetWeaver, ConnectWise at scale. Hands off credentials, persistence, and footholds to ICS-capable threat groups.

- CVE-2025-4427/4428 (Ivanti EPMM)
- Cobalt Strike, Sliver, Supershell C2
- Passes access to VOLTZITE for Stage 2 escalation

Field Data, TTX Results & Priority Actions for Electric Operators

⚠ Electric TTXs show Major Challenges in DETECT

Operators cannot reliably identify cyber activity within industrial processes before impact occurs.

2025 TTX RESULTS — ELECTRIC SECTOR

Dragos tabletop exercise performance across OT incident response capabilities

Activate	No Challenges
Detect	MAJOR Challenges
Respond	Some Challenges
Communicate	Some Challenges
Recover	No Challenges
Contain	Some Challenges
Document	Some Challenges

PRIORITY ACTIONS FOR ELECTRIC OPERATORS

1. **Remove internet exposure on cellular gateways & VFDs**
   KAMACITE specifically targeted Airlink gateways, Altivar VFDs, and Smart HMIs. If these are internet-exposed, they are on a targeting list.

2. **Build IRP scenarios for DER / CHP disruption**
   ELECTRUM struck CHP and renewable management systems in December 2025. Most utility IRPs predate this as a realistic scenario. Update them.

3. **Deploy ICS-protocol-aware monitoring**
   Monitor S7comm, Modbus, and DNP3, not just TCP/IP. VOLTZITE manipulated EWS software and dumped alarm data before detection.

4. **Eliminate default credentials on all field devices**
   35% of Electric sites still have them. BAUXITE has repeatedly exploited default credentials to gain direct OT access.

5. **Define cyber/operational anomaly escalation criteria**
   TTXs show Electric struggles with Detect. Define exactly when an unexplained operational event triggers a cybersecurity investigation.

THE FIVE ICS CYBER SECURITY CRITICAL CONTROLS

RECOMMENDATIONS

01 ICS Incident Response Plan

02 Defensible Architecture

03 ICS Network Monitoring Visibility

04 Secure Remote Access

05 Risk-based Vulnerability Management

QUESTIONS AND ANSWERS

Thank you