The State of OT Security

LSZ Production & IT

March 19, 2026

Kai Thomsen

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

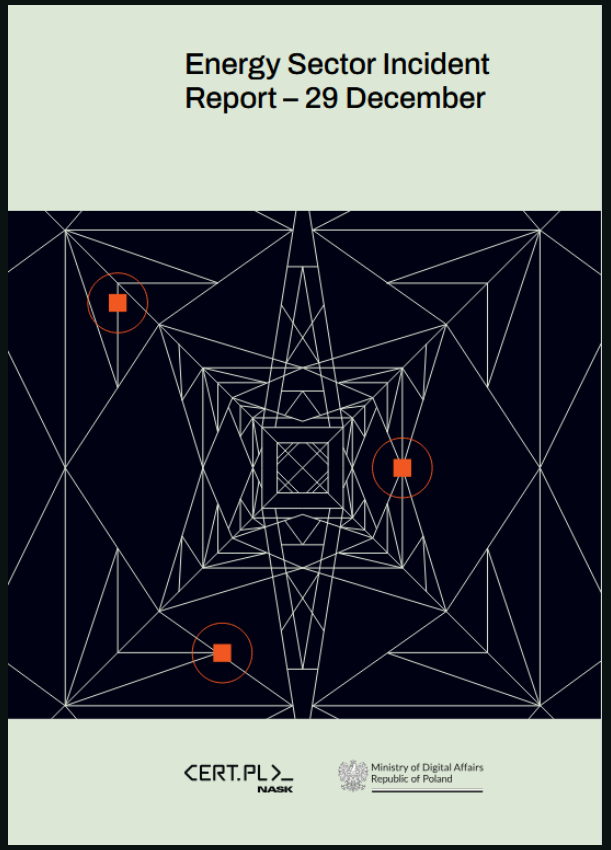
Organizations still struggle to implement basic controls, preventing an effective response when attacks occur

https://www.dragos.com/ot-cybersecurity-year-in-review

Attack Targeting DER in Poland

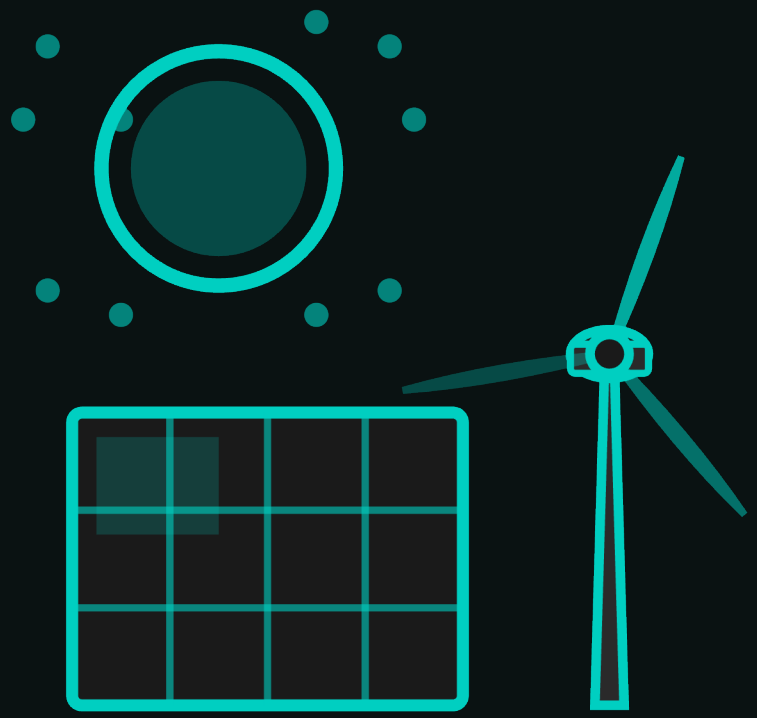
1st major attack targeting decentralized energy grids

- 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

90%

still can't detect ELECTRUM-style attacks

December 2015

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

December 2016

Deployed CRASHOVERRIDE malware against Ukrainian transmission substation affecting hundreds of thousands

2022-2025

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

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

Defenders Can’t Keep Up

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

Can't See Fast Enough

- **<5%** have PowerShell logging
- **56%** can't detect lateral movement

Can’t Respond Fast Enough

- **88%** failed detection in tabletop exercises
- **1-3 week** recovery times

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.

RECOMMENDATIONS

THE FIVE ICS CYBER SECURITY CRITICAL CONTROLS

01 ICS Incident Response Plan

02 Defensible Architecture

03 ICS Network Monitoring Visibility

04 Secure Remote Access

05 Risk-based Vulnerability Management

Q&A

QUESTIONS AND ANSWERS

kthomsen@dragos.com