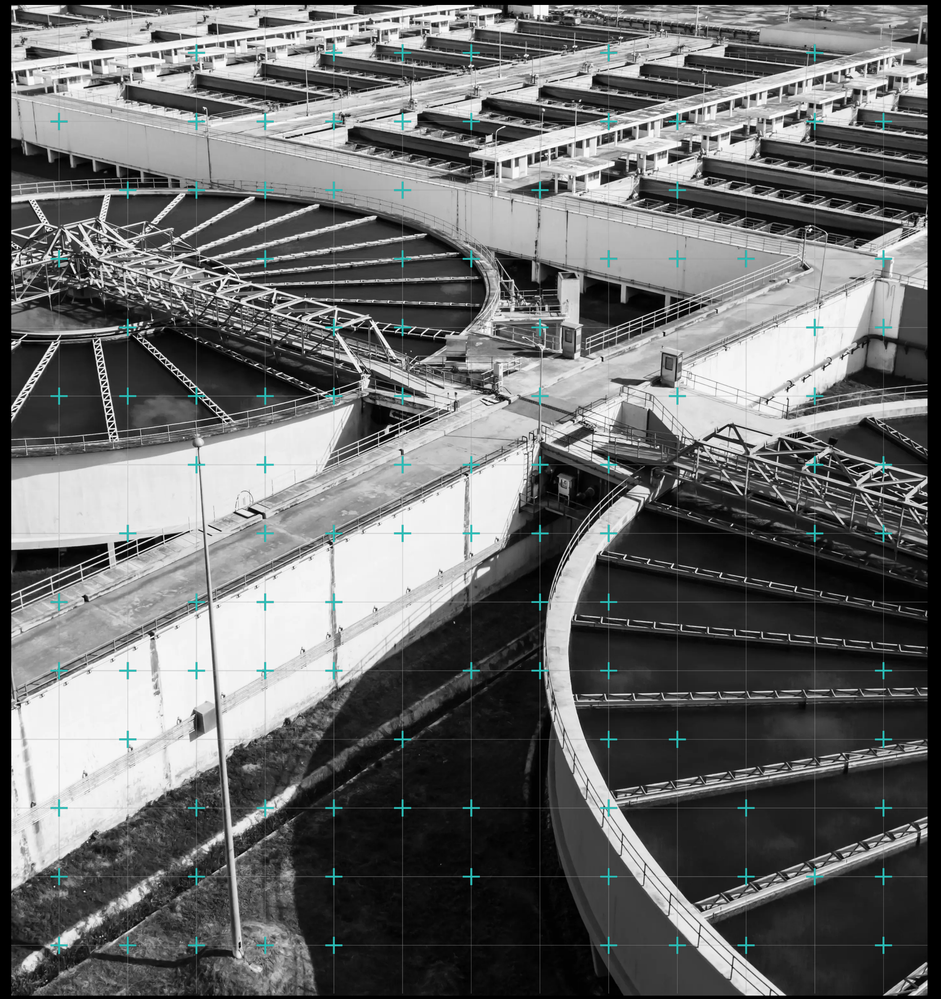
The threat landscape has expanded.

Power grids, pipelines, manufacturing plants, water facilities, and data centers now depend on systems well outside the traditional control environment

Most security programs don't cover them.

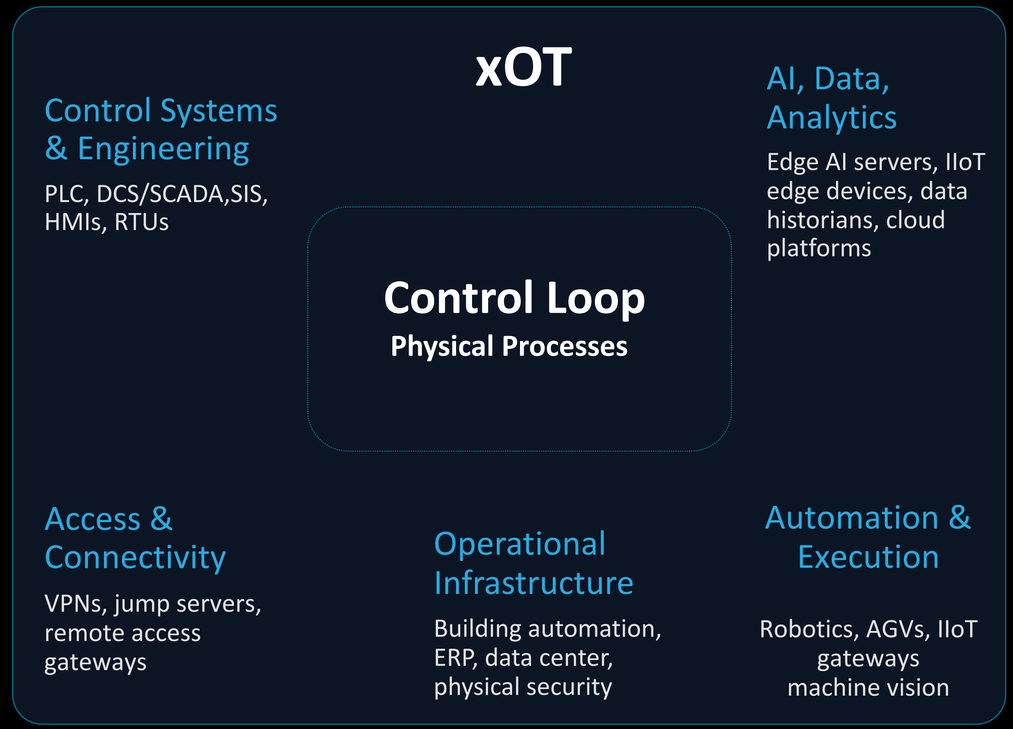


Extended Operational Technology: xOT

The full scope of what organizations need to defend

xOT is every system that influences physical processes, regardless of how it is classified, what network it sits on, or who owns it

It is the full scope of what organizations need to defend



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**

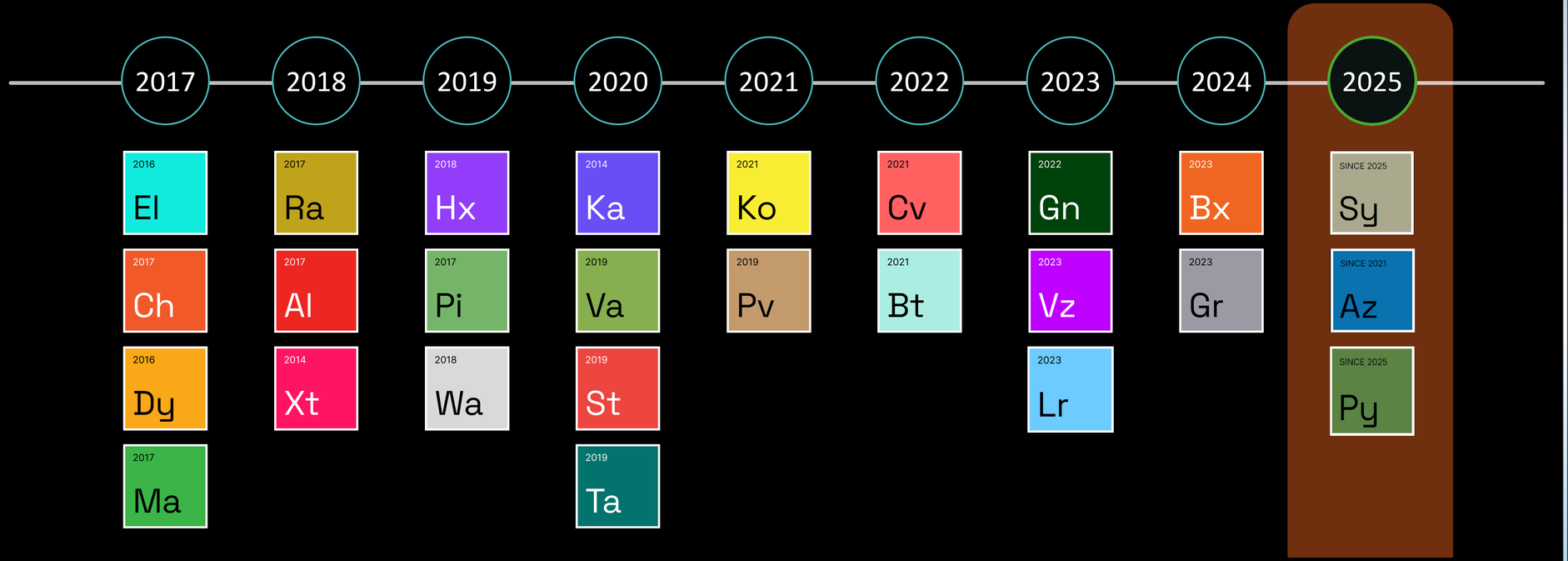
Shift from reconnaissance to **attempted operational effects throughout 2025**

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

- 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

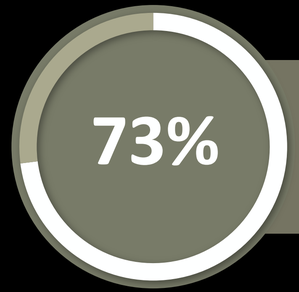
SINCE 2025

Sy

Targets:

Electric Power | Water | Oil & Gas | Manufacturing | Public Administration

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



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

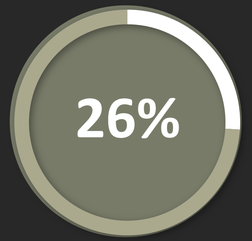
Rapid Vulnerability Exploitation Campaigns

Dec 2023 (1)
Ivanti Connect Secure CVE-2023-46805, CVE-2024-21887

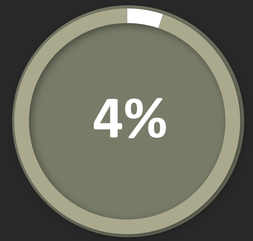
2024 (2)
F5 BIG-IP & ConnectWise ScreenConnect; F5: CVE-2023-46747; ConnectWise: CVE-2024-1709

Apr 2025 (3)
SAP NetWeaver Zero-Day CVE-2025-31324

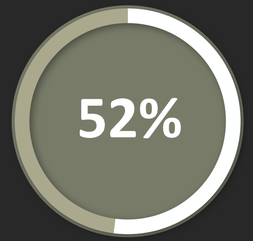
May 2025 (4)
Ivanti EPMM (U.S. Utility Victim) CVE-2025-4427, CVE-2025-4428



of advisories had NO patch when announced



had public POC & were actively exploited



Dragos provided alternate mitigations when vendors couldn't

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

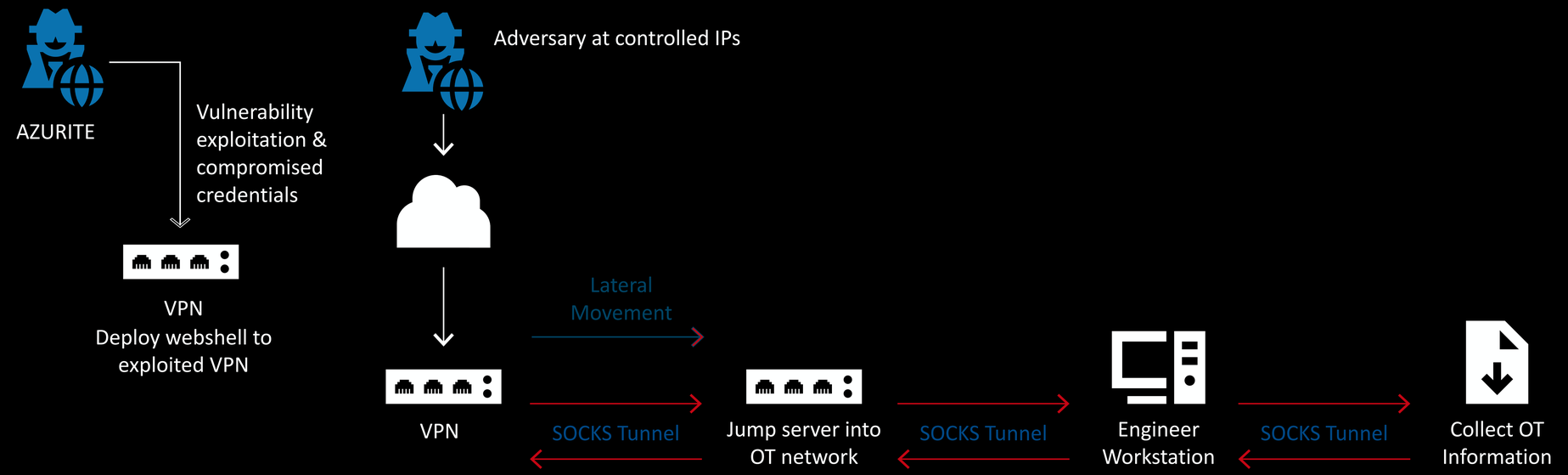
01 Exploit vulnerabilities or use VPN credentials from other credential stuffing

02 Deploy webshell to VPN device

03 Access OT jump server with compromised credentials

04 Access engineer workstation to exfiltrate OT operational information

05 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)

Expansion of KAMACITE Targets

Targeted reconnaissance & access establishment enabling ELECTRUM attacks

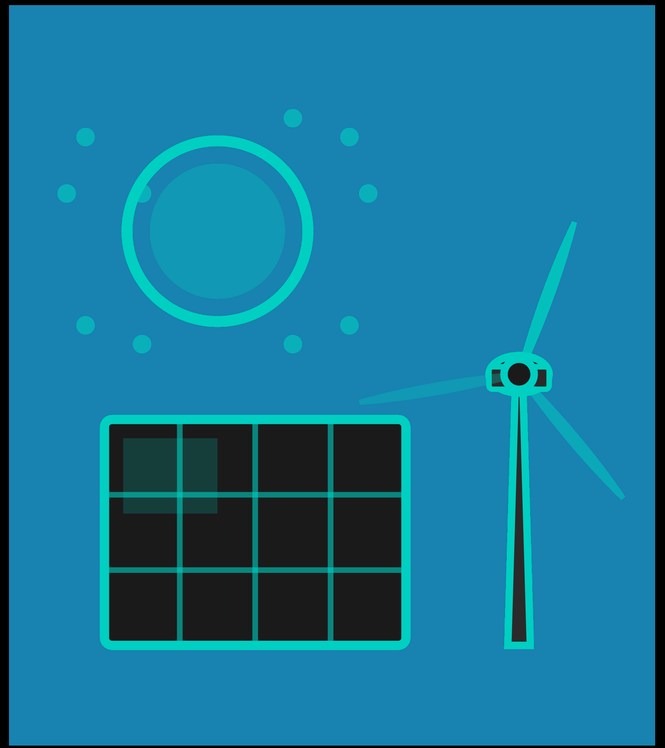
2014

Ka

- 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

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

VOLTZITE

Demonstrated capability to access
& manipulate OT/ICS assets

2023

Vz

- 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

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.

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)

Fully Functional PLC Attack Tool

Unlike IT malware, this directly commands industrial equipment to stop operating

- Forces S7-300/S7-400 PLCs to STOP mode
- Uses S7comm and COTP protocols
- Mirrors Metasploit functionality

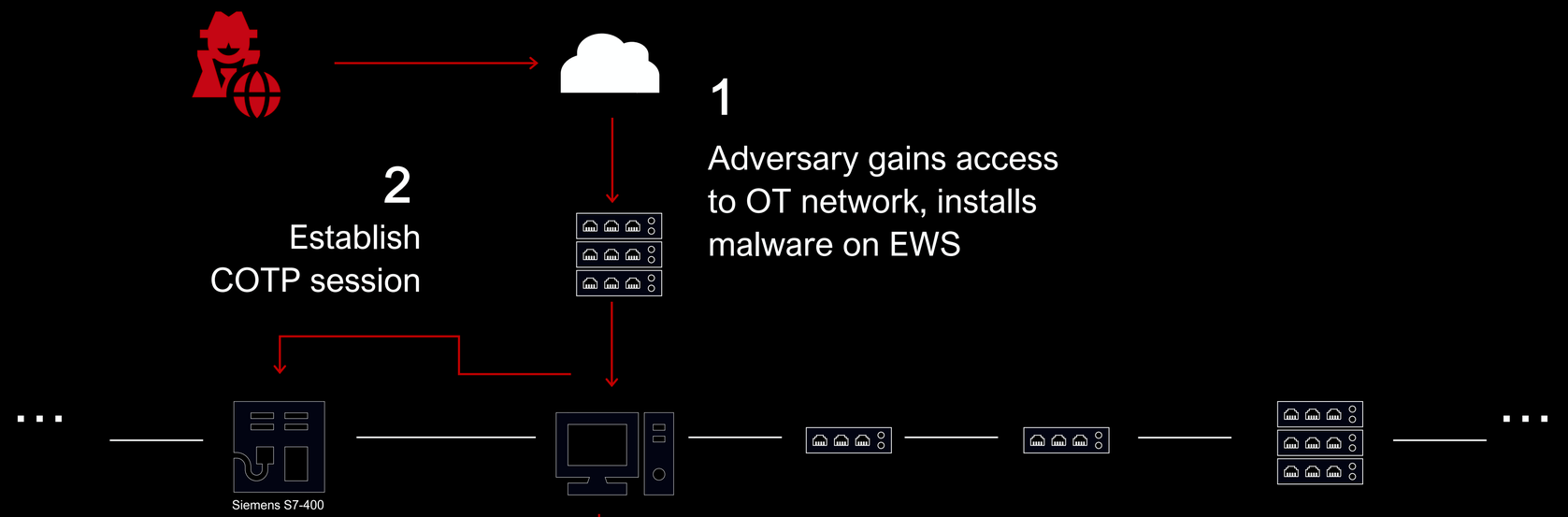
Moderate Confidence:
national red team exercise

Stage 2 Capability:
Loss of Control manufacturing, utilities, & infrastructure

45% of S7 PLCs globally are vulnerable, older models

```python
def main():
    """Main function: parse command line arguments and send command in a loop
    parser = argparse.ArgumentParser(description='S7 PLC attack tool - sends
    parser.add_argument('ip', help='PLC IP address')
    args = parser.parse_args()
    command = 'stop'
    print(f'An attack command will be sent to {args.ip} every 2 minutes')
    print('Press Ctrl+C to terminate the program')
    try:
        iteration = 1
        while True:
            print(f'\n==== Sending command iteration {iteration} ====')
            start_time = time.time()
            result = plc_control(args.ip)
            status = 'Success' if result else 'Failure'
            print(f'Command execution result: {status}')
            elapsed_time = time.time() - start_time
            wait_time = max(0, 120 - elapsed_time)
            time.sleep(wait_time)
            iteration += 1
```

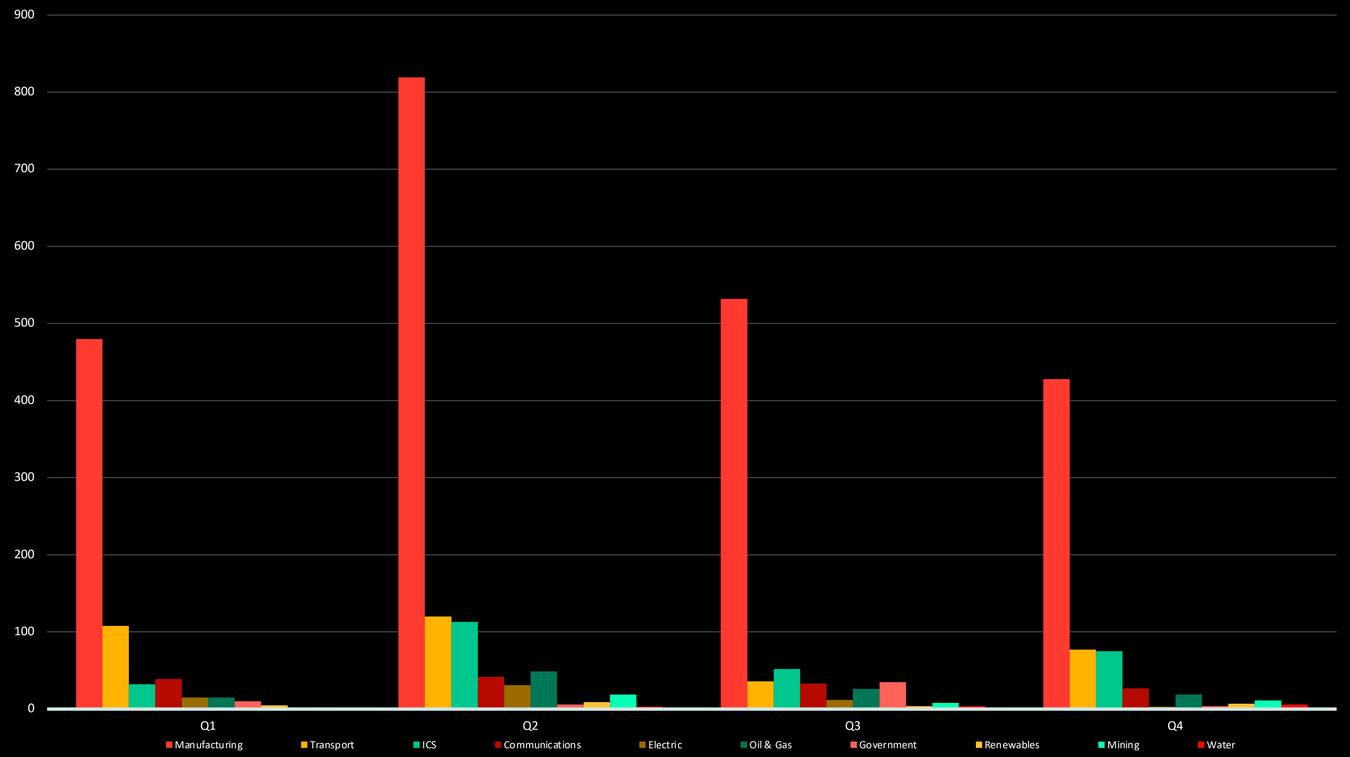
PLC_Controller.exe Attack Path



COTP = Connection-Oriented Transport Protocol
EWS = Engineering Workstation
PLC = Programmable Logic Controller

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.

OT was never about the operating system: The point is the physical process

“It only hit Windows systems.”

Engineering workstations run Windows. HMIs run Windows. Historians run Windows.

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

Mexico Municipal Water Utility

AI as intrusion tool: commercial model used against OT infrastructure at scale

- An adversary with no prior OT knowledge tasked commercial AI to conduct post-compromise discovery
- Within hours, the AI identified a SCADA-adjacent industrial gateway and assessed it as a high-value target

- AI iteratively built and refined a 17,000-line intrusion framework in near-real time
- Compressed tooling development from weeks to hours

- AI executed an automated credential spray against a single-factor OT authentication interface
- The world of IT adversaries being told to target OT will increase the frequency of incidents we experience

Dragos assisted Gambit Security investigation, Q1 2026. Full technical analysis: Dragos.com

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

THANK YOU