Dragos 2026 OT Cybersecurity Report

Year in Review Overview

Oliver Herterich
Principal Solution Architect / IR / TH

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

DRAGOS

620+ EMPLOYEES

580+ CUSTOMERS

28 COUNTRIES

11 INDUSTRY VERTICALS

Built For Practitioners, By Practitioners

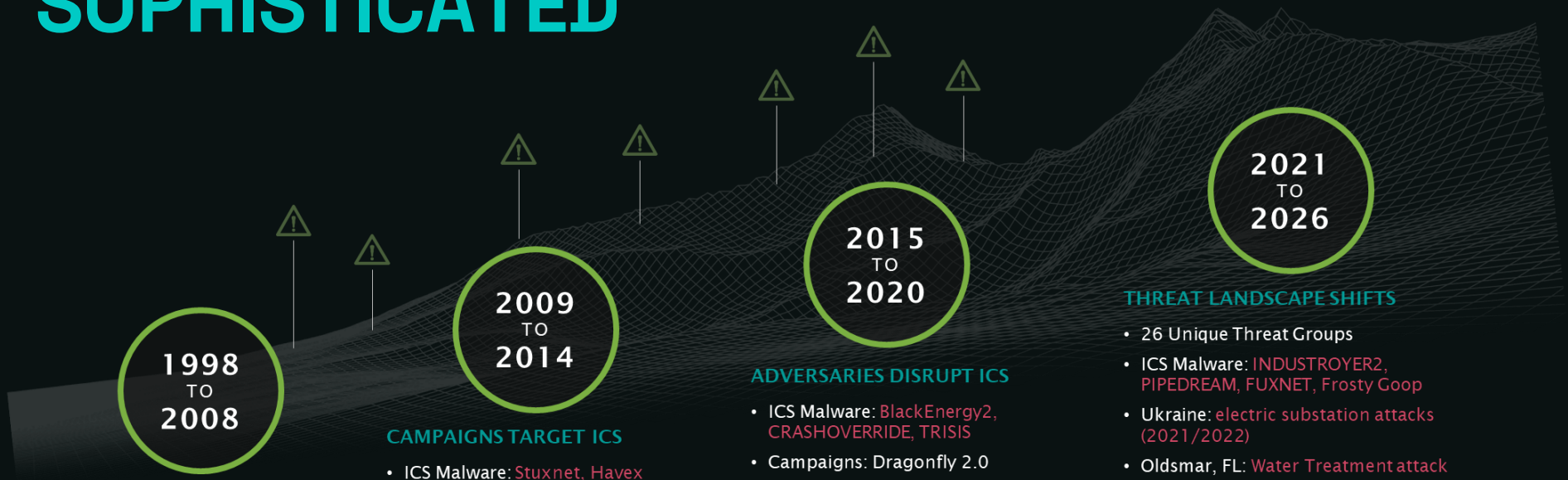
The largest & most experienced team of ICS security specialists make the best technology.

- ELECTRIC
- WATER
- OIL & GAS
- FOOD & BEV
- MANUFACTURING
- MINING
- BLDG AUTO SYS
- TRANSPORTATION
- CHEMICAL
- PHARMACEUTICAL
- GOVERNMENT

HQ | Hanover, MD

REGIONAL | US & Canada, Australia-New Zealand, Gulf Coast, UK/Europe, Singapore, Japan

OT THREATS MORE FREQUENT & SOPHISTICATED



LACK OF COLLECTION

- Campaigns: APT1
- ICS Malware: None

CAMPAIGNS TARGET ICS

- ICS Malware: Stuxnet, Havex
- Campaigns: Sandworm, Dragonfly
- Ukraine: Germany: 1st attack cause physical destruction on civilian infrastructure (steel)

ADVERSARIES DISRUPT ICS

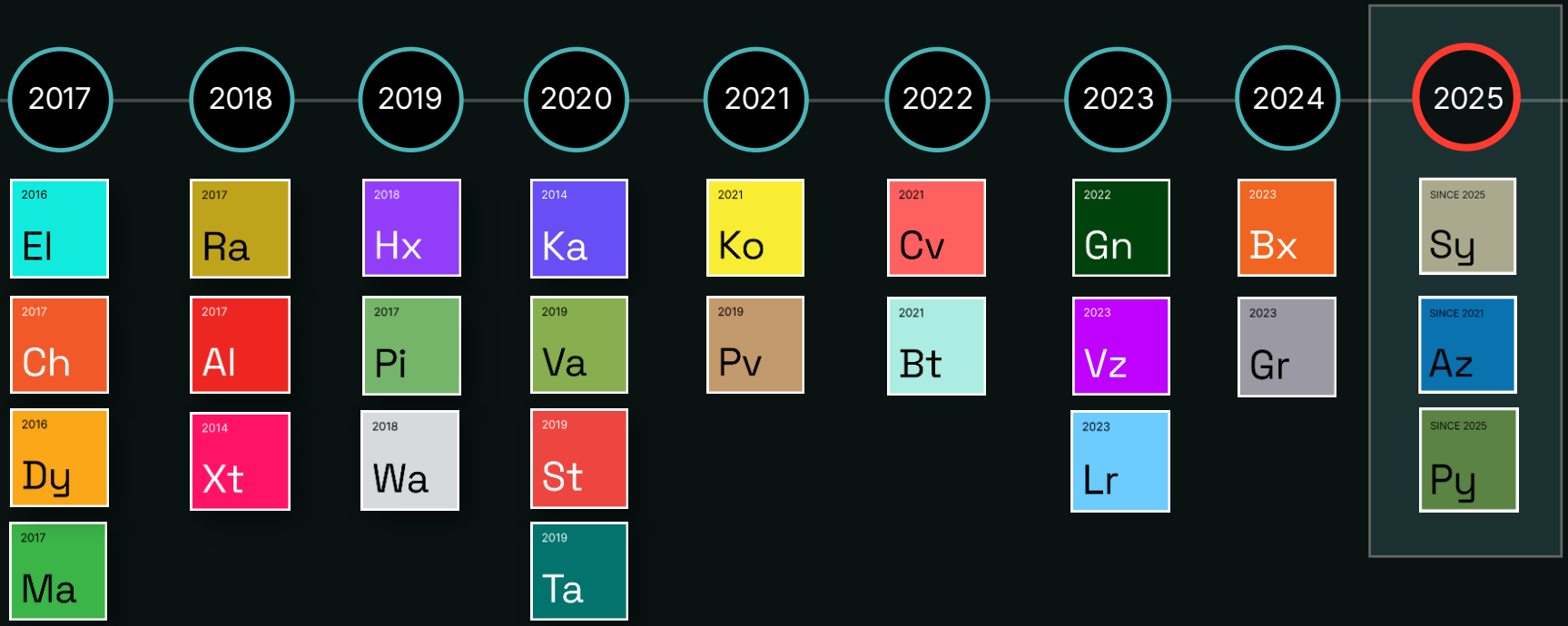
- ICS Malware: BlackEnergy2, CRASHOVERRIDE, TRISIS
- Campaigns: Dragonfly 2.0
- Ukraine: disruption of electric power operations (2015), major electric grid disruption (2016)
- Saudi Arabia: first attack targeting human life (2017)

THREAT LANDSCAPE SHIFTS

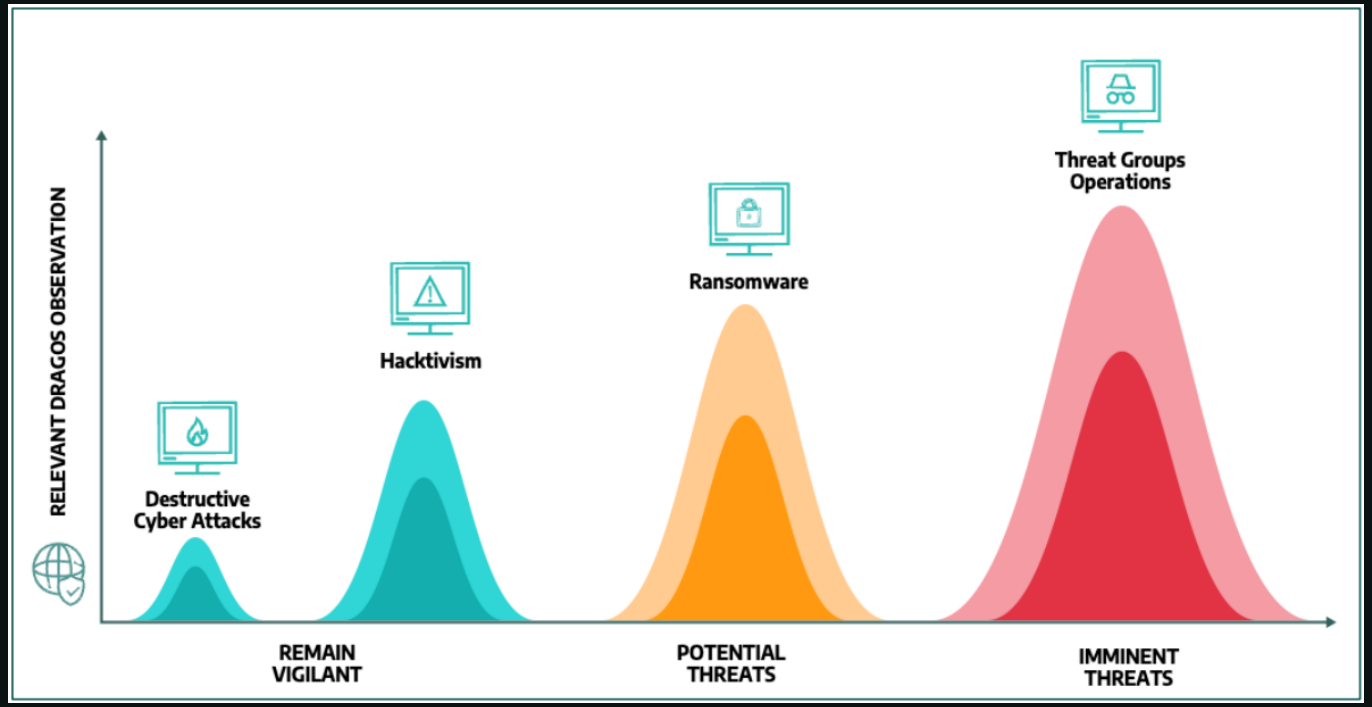
- 26 Unique Threat Groups
- ICS Malware: INDUSTROYER2, PIPEDREAM, FUXNET, Frosty Goop
- Ukraine: electric substation attacks (2021/2022)
- Oldsmar, FL: Water Treatment attack
- Hacktivist Attacks: disruption of water utilities in U.S., Europe (2023)
- Ransomware attacks: Colonial Pipeline, JBS Foods, Norsk Hydro, Kojima, Foxconn, Dole, Yanfeng Automotive, Boeing

Dragos Identifies 3 New Threat Groups

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

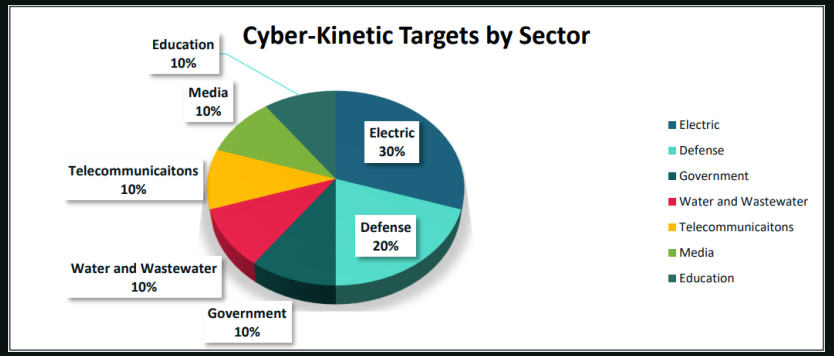


THREAT ACTORS



CONFLICT-DRIVEN CYBER-KINETIC TACTICS

- Prior to, in conjunction with or as a response to kinetic action
- Cyber operations used to:
  - interrupt communications,
  - disrupt government and military coordination,
  - instill psychological impacts,
  - Identify organizational weaknesses in critical industries
  - test defensive response capabilities



TACTICS, TOOLS, & PROCEDURES - TRENDS

New ICS Malware
with growing adversary knowledge expose detection gaps in OT.

Internet-accessible OT devices
key attack path, highlighting need for simple changes to create more defensible architectures

Remote Access
adversaries routinely exploit VPNs, SSH, default credentials, & third-party remote access.

Lateral Spread After Compromise
adversaries use LOTL techniques, native tools, ICS protocols to evade detection.

THREAT GROUP UPDATE

NEW: SYLVANITE

Rapid exploitation broker enabling VOLTZITE access to critical infrastructure

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

Targets: Electric Power, Water, Oil & Gas, Manufacturing, Public Administration

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

73%

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

Rapid Vulnerability Exploitation Campaigns

1. **Dec 2023:** Ivanti Connect Secure CVE-2023-46805, CVE-2024-21887
2. **2024:** F5 BIG-IP & ConnectWise ScreenConnect; F5: CVE-2023-46747; ConnectWise: CVE-2024-1709
3. **Apr 2025:** SAP NetWeaver Zero-Day CVE-2025-31324
4. **May 2025:** Ivanti EPMM (U.S. Utility Victim) CVE-2025-4427, CVE-2025-4428

26% of advisories had NO patch when announced

4% had public POC & were actively exploited

52% Dragos provided alternate mitigations when vendors couldn't

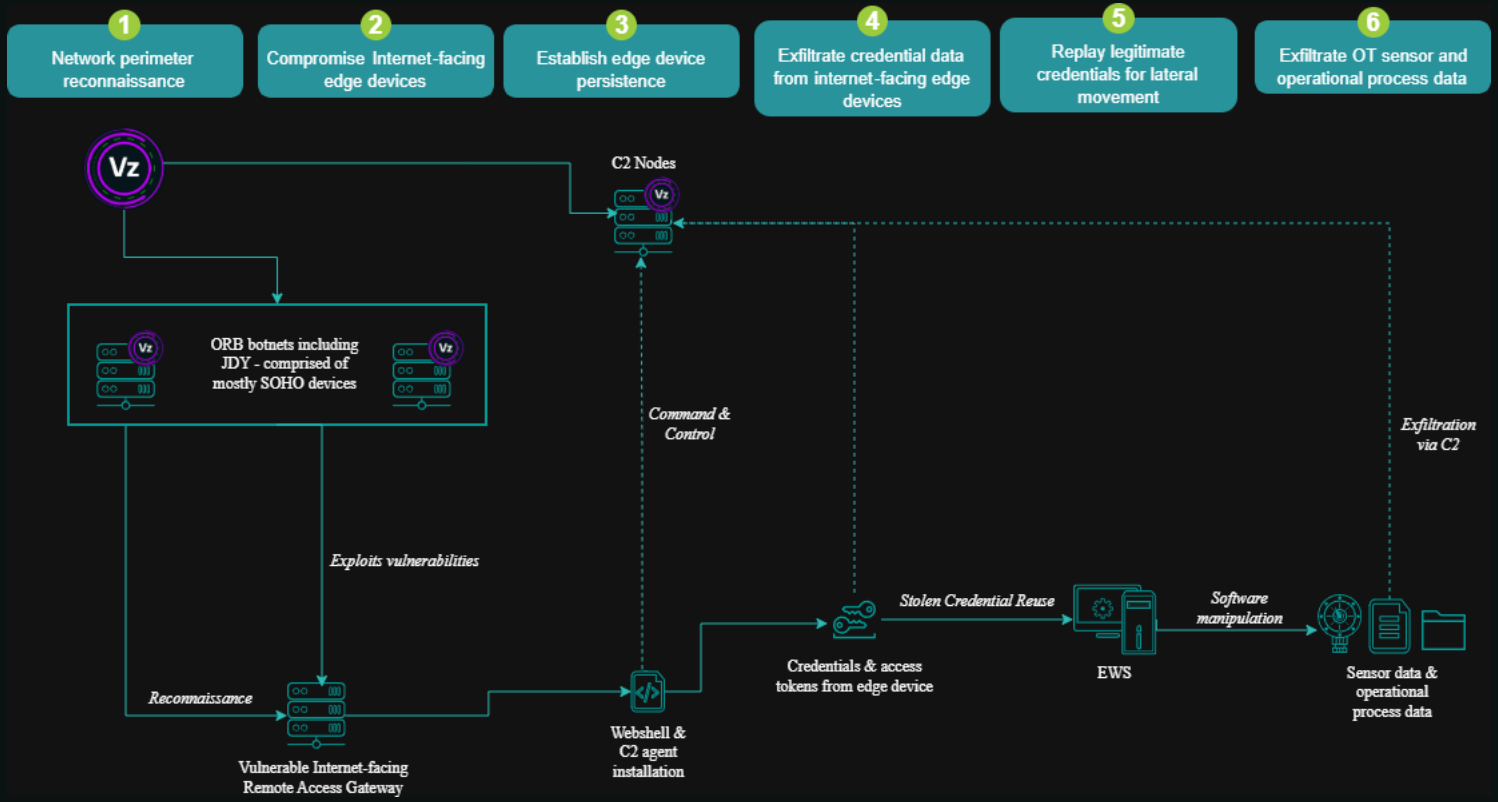
VOLTZITE

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



NEW: AZURITE

Theft of operational information, long-term access enablement

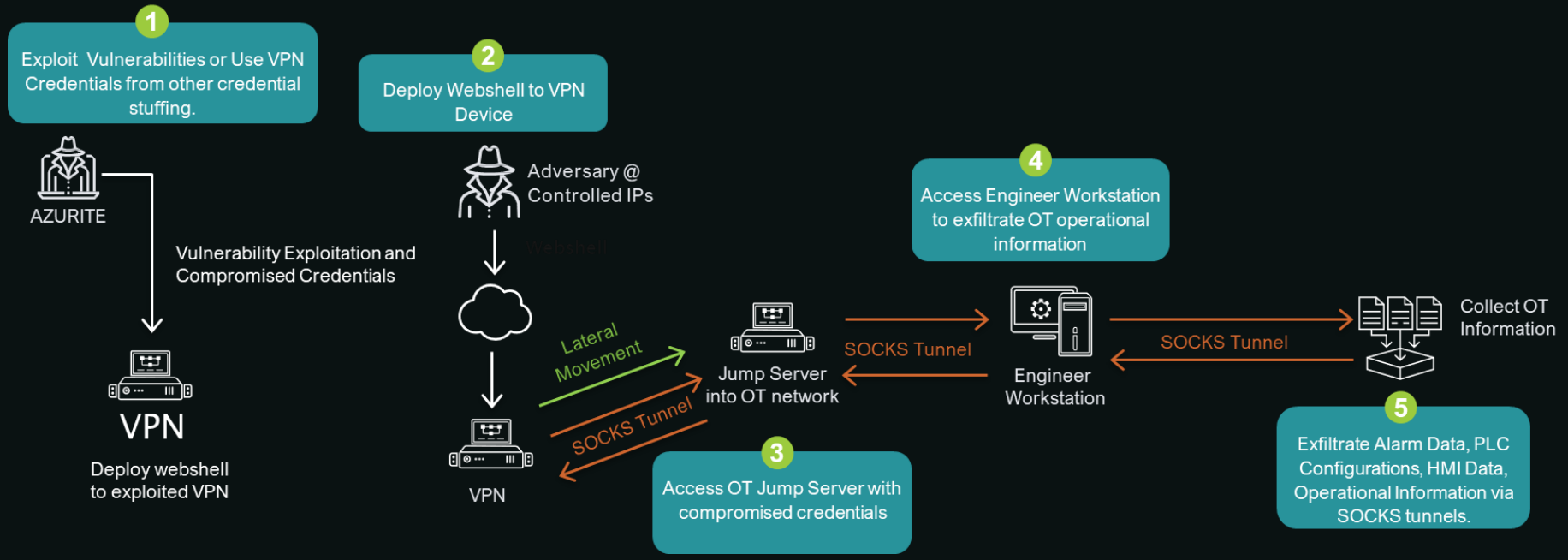
What Dragos Observed in 2025

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

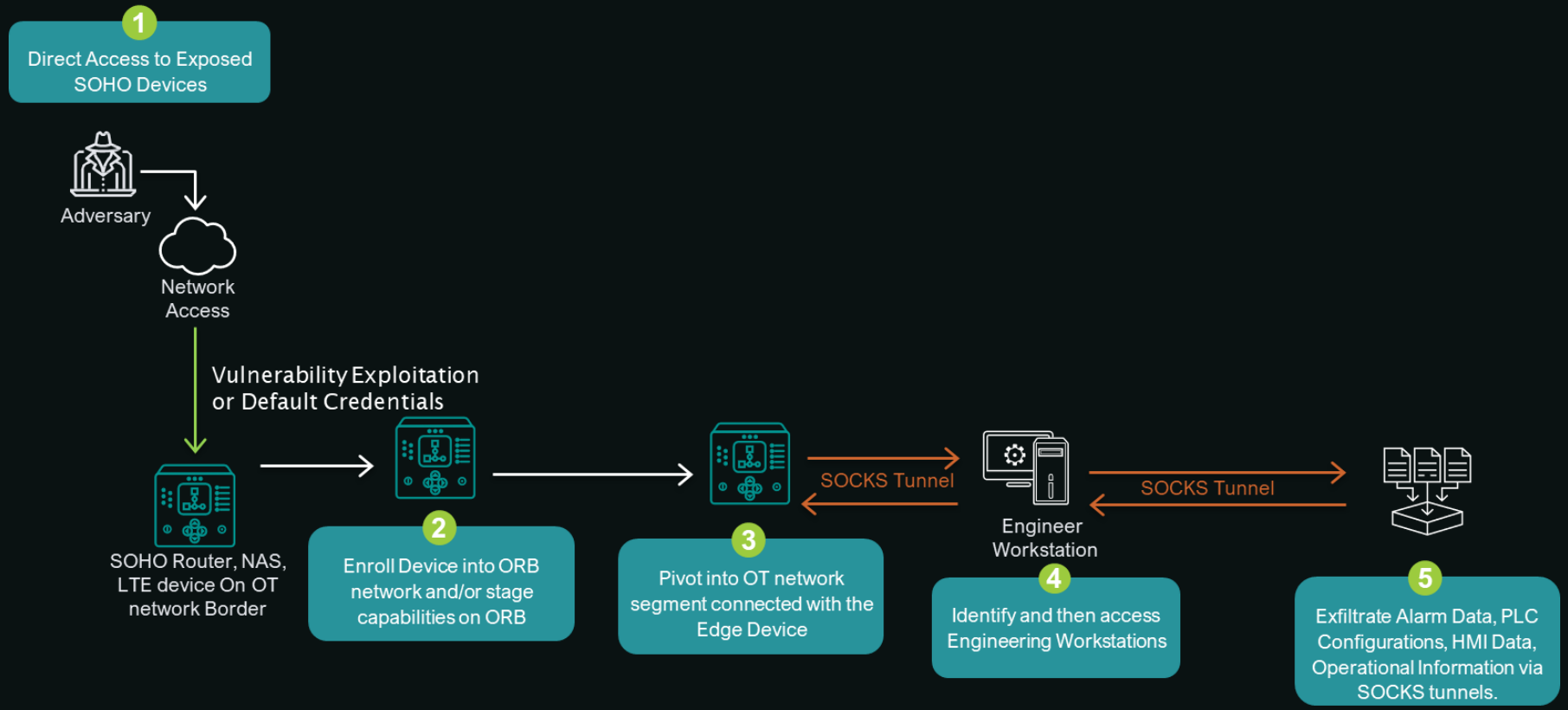
Targets: Manufacturing, Defense, Automotive, Electric, Government, Oil & Gas

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

AZURITE: VPN Access to OT Environment and Engineer Workstation

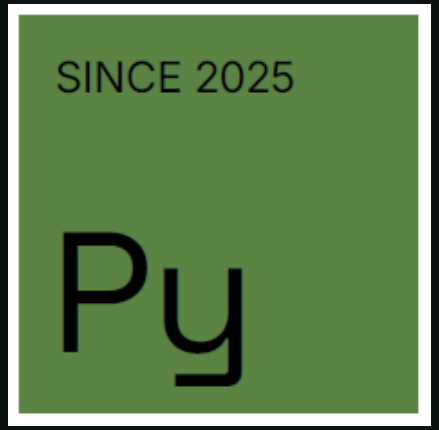


AZURITE: SOHO Device Compromise to Achieve OT Access



NEW: PYROXENE

Cross-domain access enabling movement from IT into OT networks



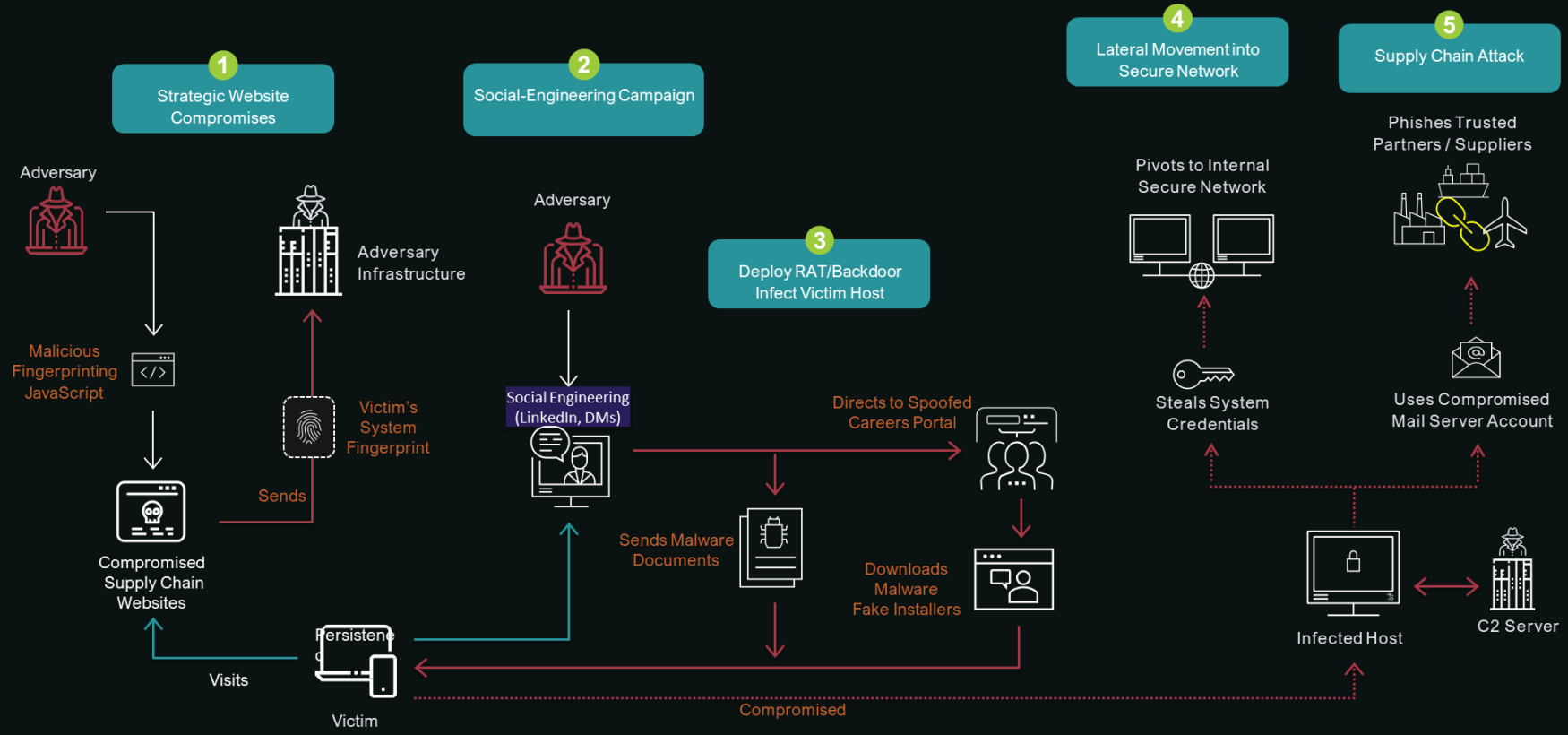
What Dragos Observed in 2025

- Created fake LinkedIn profiles posing as aerospace recruiters
- Compromised defense contractor websites to target employees
- Used stolen credentials to access Citrix and VMware systems
- 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



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)

Systematically targeted:

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

Also Observed:

VOLTZITE: Dumps configs to find process stop triggers

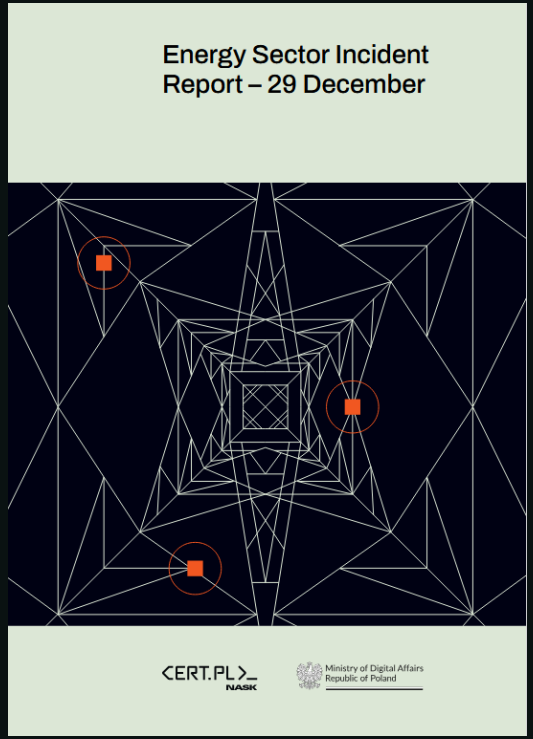
AZURITE: Exfiltrates alarm data for operational boundaries

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

Attack Targeting DER in Poland

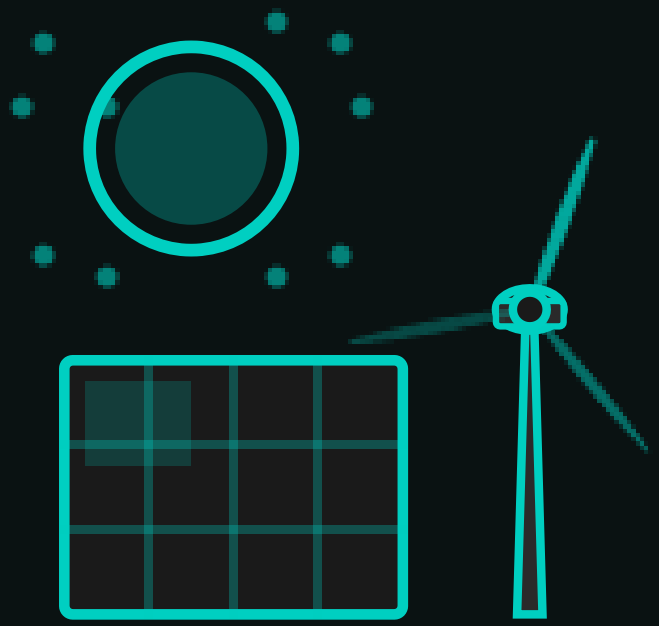
1st major attack targeting decentralized energy grids

- 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 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 SoIntsepek hacktivist persona
- New destructive wiper variant, continuing toolkit evolution

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

BAUXITE

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

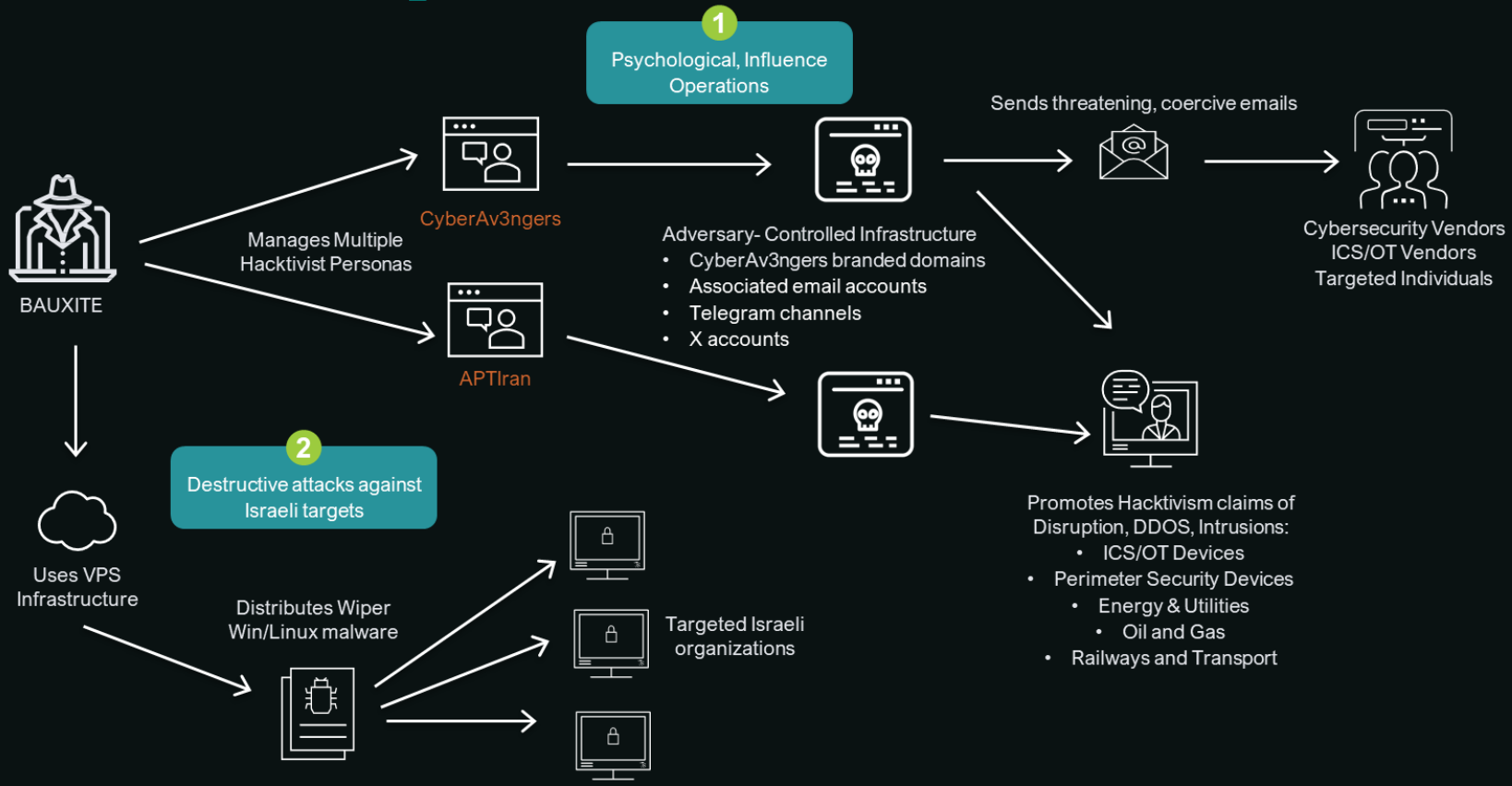
What Dragos Observed in 2025

- 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

Operates as: CyberAv3ngers (hacktivist persona)

BAUXITE 2025 Activity



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

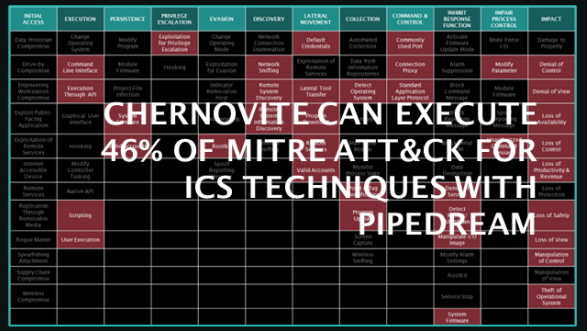
Malware

CHERNOVITE'S PIPEDREAM MALWARE

1st scalable, cross-industry OT attack toolkit

7th ICS/OT targeting malware

Discovered before it was employed for destructive purposes



EVILSCHOLAR & BADOMEN
are extensible – this is rare.

1000s of CODESYS devices across multiple sectors at risk

MOUSEHOLE
manipulates OPC-UA server nodes & associated devices.

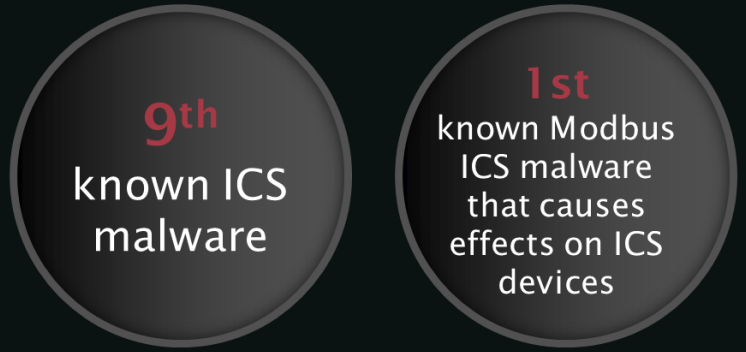
OPC-UA is a widely used communication protocol in ICS/OT

DUSTTUNNEL & LAZYCARGO
demonstrate that CHERNOVITE can achieve an end-to-end attack.

FROSTYGOOP ICS MALWARE

What happened?

- In January 2024, during sub-zero temperatures, a cyber attack disrupted the energy supply for central heating in more than 600 apartment buildings in Ukraine.
- The adversaries possibly gained access to the victim's network in April 2023 using an undetermined vulnerability in Mikrotik routers.
- The adversary sent Modbus (TCP/502) commands directly to the district heating system's ENCO controllers.



46,000

Internet-exposed ICS devices communicating over Modbus

Modbus is used worldwide across industries.

HACKTIVISM

TRADITIONAL HACKTIVISM MOTIVATION

FUD

Fear, **U**ncertainty, **D**oubt

Draw attention to geopolitical and social causes.
Influencing perceptions to create a narrative of instability.

- DDoS attack


- Website defacement

- False claims

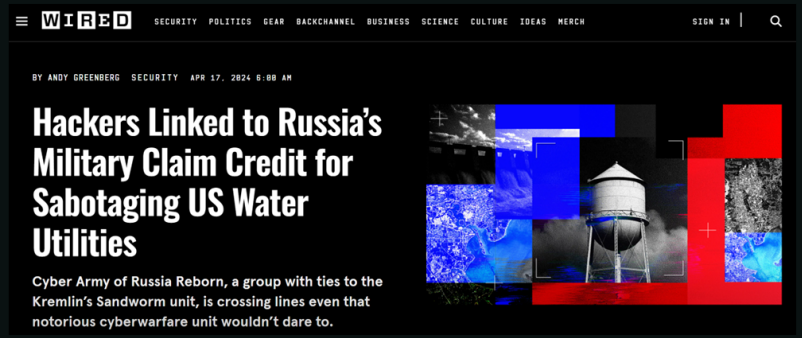

THE RISE OF CONFLICT-DRIVEN HACKTIVISTS

MOTIVATED BY UKRAINE-RUSSIA WAR

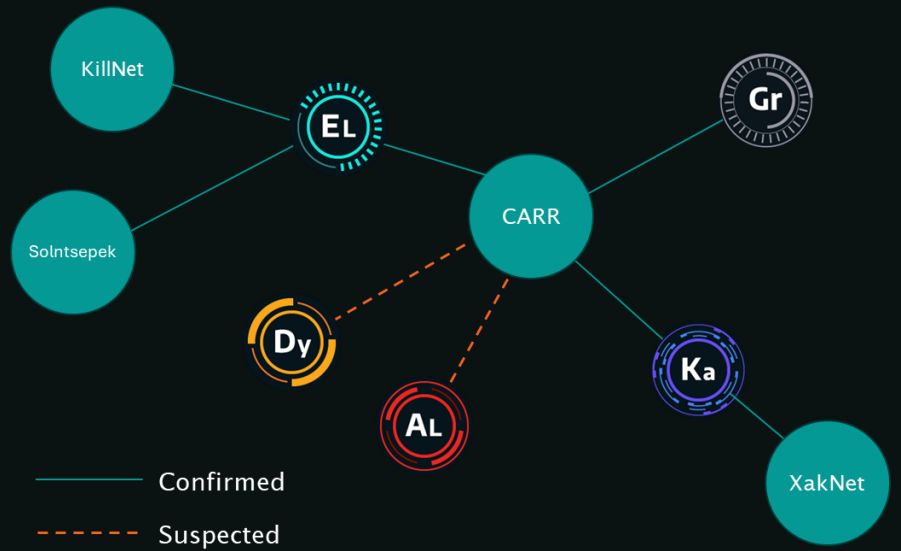
GhostSec
Proukraine
Zarya
Name057(16)
Anonymous Sudan
Killnet
SiegedSec
CyberArmyofRussia_Reborn

MOTIVATED BY ISRAEL-HAMAS CONFLICT

Cyber Av3ngers
ThreatSec
AnonGhost
Predatory Sparrow



CONVERGENCE OF HACKTIVISM & STATE-SPONSORED THREATS



Shared Infrastructure

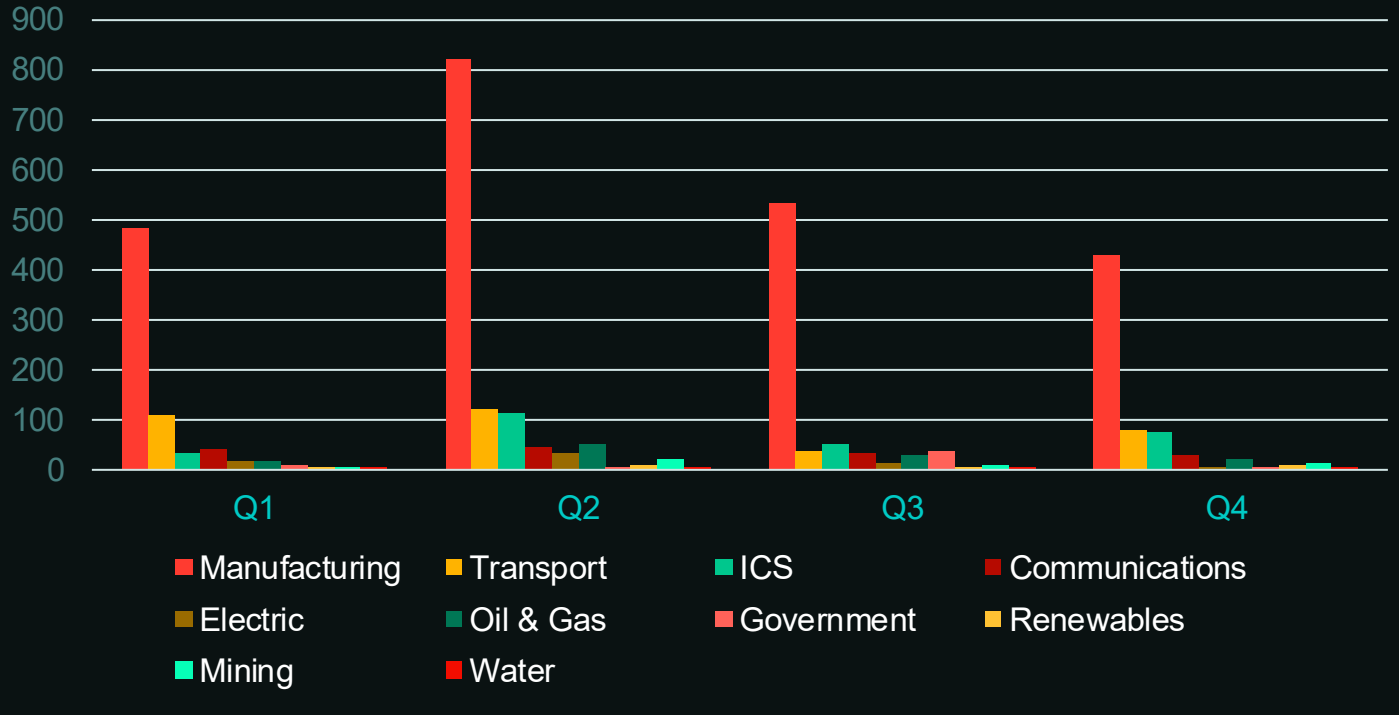
Intelligence Sharing

Victim Overlaps

RANSOMWARE

Ransomware by Sector

In 2025, 3318 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."

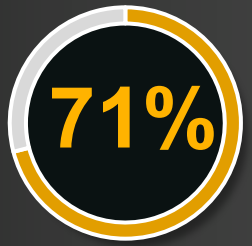
Engineering workstations run Windows. HMIs run Windows. Historians run Windows.

VULNERABILITY

Necessity of Risk-Based Decision

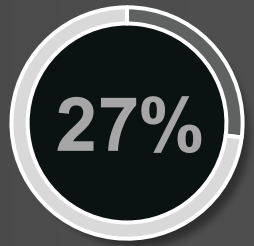
Only some vulnerabilities need immediate action

of ICS/OT vulnerabilities needed to be addressed



are network exploitable with no direct operational impact

These need to be addressed



pose a possible threat but rarely require action

They likely never need to be addressed

NOW

NEXT

Mitigate through network monitoring, segmentation & MFA

NEVER

Monitor these for signs of exploitation

PRACTICAL RISK MITIGATION IN ICS/OT

PATCHING CAN BE IMPRACTICAL IN ICS/OT DUE TO SAFETY & PRODUCTION REQUIREMENTS, ALTERNATIVE MITIGATION IS KEY

74%
Advisories with a patch

26%
Advisories with no patch when announced

47%
DRAGOS PROVIDED ALTERNATE MITIGATIONS FOR ADVISORIES MISSING BOTH A PATCH & MITIGATIONS

RECOMMENDATIONS

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

Thank you
oherterich@dragos.com