Emerging Trends in OT: Staying ahead of Cyber Threats in 2026

9th December 2025

Together we're creating
a more secure digital future

Agenda

- **Introduction**
- **Threat Landscape Briefing**
- **Lessons Learned & Emerging Trends**
- **Building a Proactive OT Cyber Resilience Strategy in 2026**
  - Moving from reactive to proactive defence
  - Intelligence-led threat detection
  - Incident readiness best practices
- **Live Q&A**

Meet our Panel

David Brown

Principal Security Consultant (DFIR), NCC Group

Matt Hull

Global Threat Intelligence Lead, NCC Group

Magpie Graham

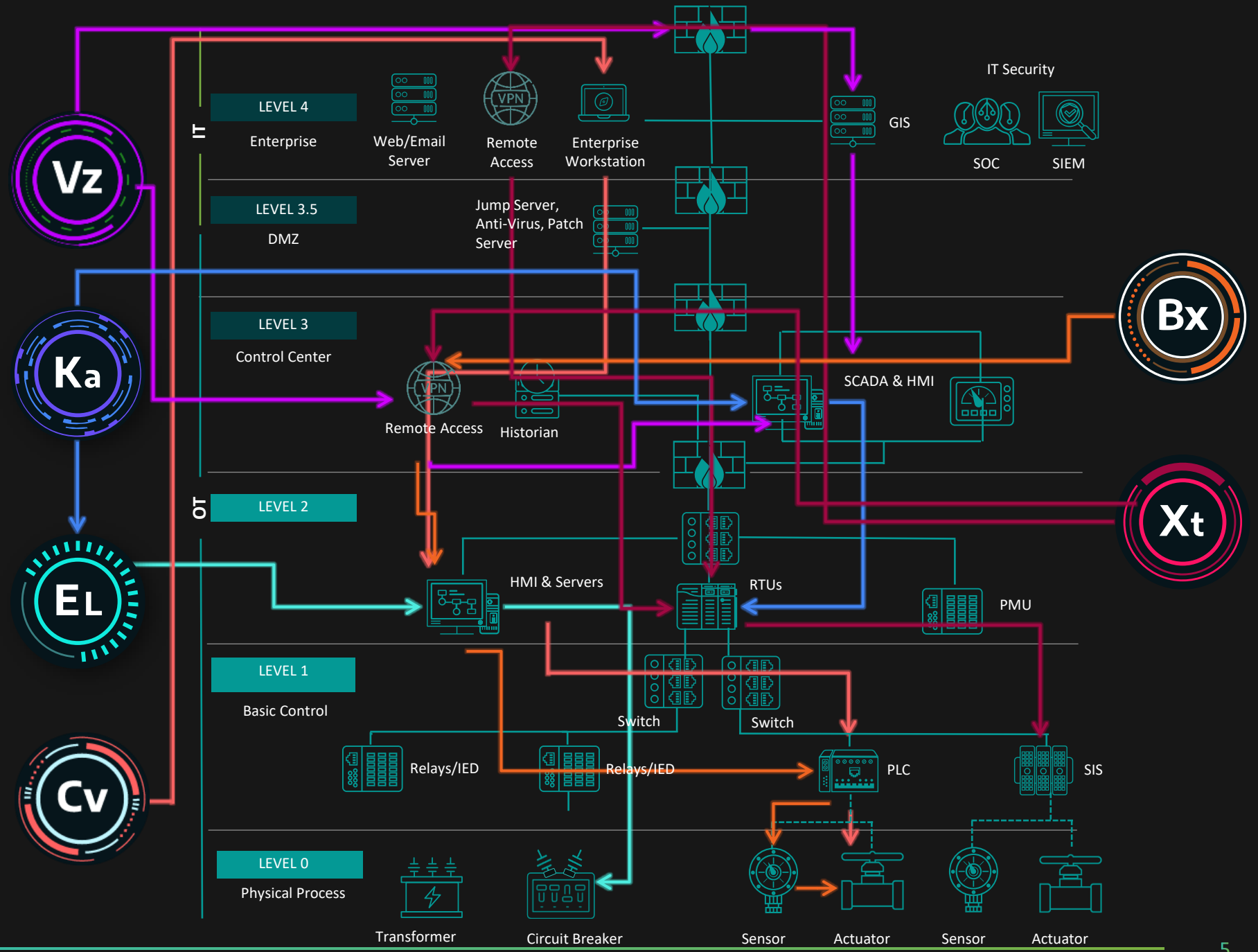
Technical Director of Intel & Services, Dragos

OT Threat Landscape Briefing

Emerging Trends in OT: Staying ahead of Cyber Threats in 2026

Why OT Monitoring is Critical

- Threat groups are targeting operational technology
- They employ techniques that circumvent traditional network perimeter-based and device level security controls



VOLTZITE

Heavy use of living off the land (LOTL) and living off the network (LOTN) techniques, evading detection with use of captured credentials, compromised assets.

Kill Chain

Delivery	STAGE 01
Exploit	STAGE 01
Install/Modify	STAGE 01
C2	STAGE 01
Act	STAGE 01

Intent

Espionage for operational information exfiltration, long-term persistent access, and intelligence preparation of the environment.

Targets

Electric Power Generation, Transmission & Distribution,
Oil and Gas Midstream & Downstream,
Emergency Services, Telecommunications,
Defense Industrial Base, Military,
SLTT, Utilities, Satellite Services

Observed VOLTZITE Campaigns

Compromised Oil and Gas Organizations by exploiting end-of-life Sierra Wireless AirLink Raven Devices to conduct process control manipulation.

Compromised Utilities in Major Metropolitan Areas and exfiltrated operational data, process information, and business continuity procedures.

Compromised Utilities near United States Military Bases by exploiting perimeter access devices to gather info on water systems and operations.

Exploited Perimeter Devices to access Defense Industrial Base organizations.

GRAPHITE

SPEAR-PHISHING, CREDENTIAL CAPTURE

Custom script-based malware

Exploitation of CVE-2023-23397 (Outlook), CVE-2023-38831 (WinRAR).

Focused on exfiltration & credential capture.

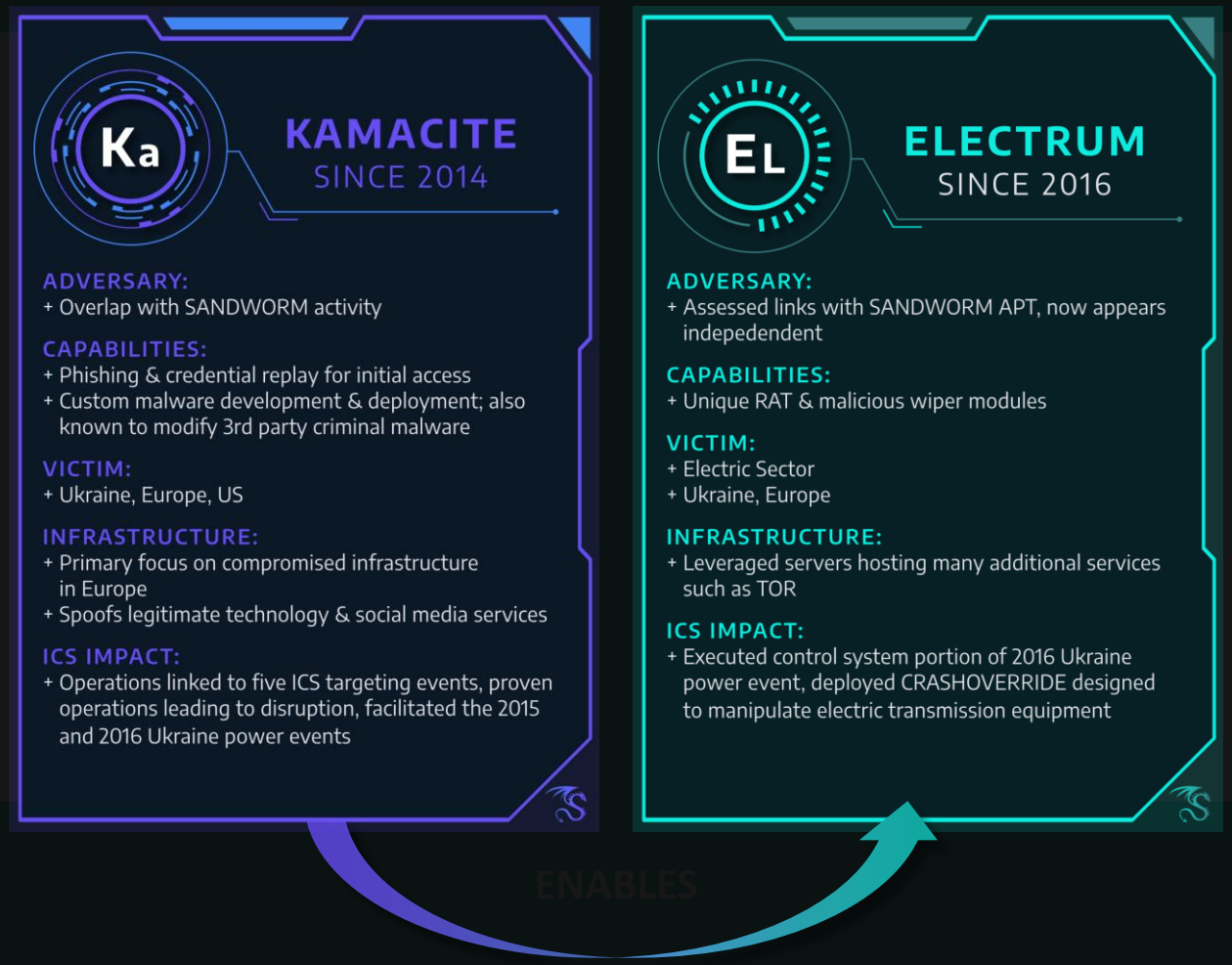
- Oil & Natural Gas
- Electric
- Defense Suppliers
- Government

Update: KAMACITE: & ELECTRUM

CONTINUED PARTNERSHIP, KAMACITE ENABLES ELECTRUM ICS ATTACKS

KAMACITE

- Persistent intrusions into Ukraine critical infrastructure, including energy & telecom networks.
- New Kapeka malware used to exfiltrate data and maintain persistent access.
- Activity observed expanding to European oil & gas sectors, using SSH brute-force techniques.



ELECTRUM

- Key player in the Kyivstar telecom attack (March 2024), disrupting telecommunication & critical infrastructure communication systems.
- Focus on energy grids & communication infrastructure in Ukraine & Poland.
- Increased use of OT-aware malware designed to manipulate ICS.

Stage 2 ICS Cyber Kill Chain

Modification of PLC Logic

BAUXITE Unitronics Attacks: downloaded malicious logic to Unitronics PLCs, caused DoS, halted industrial processes.

ICS Protocol Abuse

FrostyGoop malware: sent crafted Modbus TCP commands to alter sensor readings, resulted in heating outages.

Wiper Malware Targeting ICS Devices

ELECTRUM AcidPour Wiper: designed to wipe embedded devices running Linux in OT environments, focused on disabling operational functionality.

TTP Trends

- Use of native ICS Protocols (Modbus, s7comm, OPC/UA)
- Deployment of custom malware on OT systems
- Targeted Disruption: Loss of View, Loss of Control, Denial of Service
- Stealthy execution using LOTL techniques

DEFENDER TAKEAWAYS

Implement ICS protocol aware monitoring.

Monitor changes to PLC configurations.

Restrict external access to critical control systems.

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.

Dragos discovered FrostyGoop in April 2024.

FrostyGoop interacts directly with industrial control systems (ICS) using Modbus TCP over port 502.

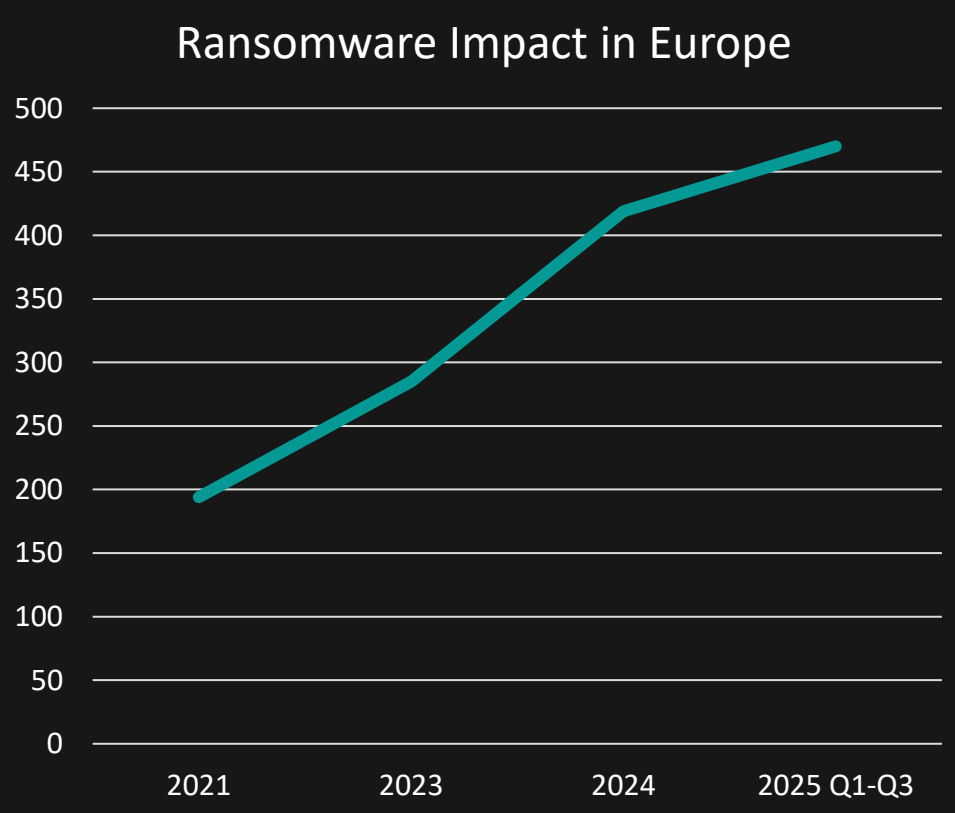
9th
known ICS malware

1st
known Modbus ICS malware that causes effects on ICS devices

46,000
Internet-exposed ICS devices communicating over Modbus TCP

Modbus is used worldwide across industries.

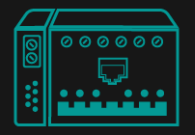
RANSOMWARE IMPACT



Global Sector Impact 2025 Q1-Q3

Manufacturing
1440

Transport
221



ICS
159

Telecom
99

Oil & Gas
60

Government
49

Electric
30

Mining
21

Renewables
16

Water
12

Lessons Learned from the OT Threat Landscape

Building a Proactive OT Cyber Resilience Strategy in 2026

Emerging Trends in OT: Staying ahead of Cyber Threats in 2026

Recommendations

01 ICS Incident Response Plan

02 Defensible Architecture

03 ICS Network Monitoring Visibility

04 Secure Remote Access

05 Risk-based Vulnerability Management

Key Takeaways

OT Attack Patterns Are Shifting

Adversaries are shifting from IT-centric attacks to OT-specific techniques, targeting lower-level devices like PLCs and HMIs.

Visibility Is Non-Negotiable

Asset discovery and continuous monitoring remain the foundation for resilience—know what you have before you can defend it.

Defence Driven by Intelligence

Map threat intel to detection rules and tune regularly; proactive measures reduce dwell time and improve incident response.

Resilience Requires Governance

Align people, process, and technology with frameworks like the SANS 5 Critical Controls to ensure integrity and continuity.

Q&A

Ask a question to our panel.

Thank you.

Together we're creating a more secure digital future