Securing OT in Transport & Logistics

Five critical controls to address the moving threat landscape

Tuesday, 12 September 2023

Josh Hanrahan

Principal Adversary Hunter

Global Electric Industry Focused Adversary Hunter

Previous:

- Lead Threat Hunter @ Commonwealth Bank
- Threat Intelligence Analyst @ Australian Energy Market Operator (AEMO)

Certs:

- GIAC Certified Forensic Analyst (GCFA)
- GIAC Reverse Engineering Malware (GREM)
- GIAC Cyber Threat Intelligence (GCTI)
- Bachelor of Information Technology (BInfoTech)
- Graduate Certificate in Cyber Security (GradCertCyberSec)

Contact:

- jhanrahan@dragos.com
- @cyberbubblez
- Nocht.org

Objective

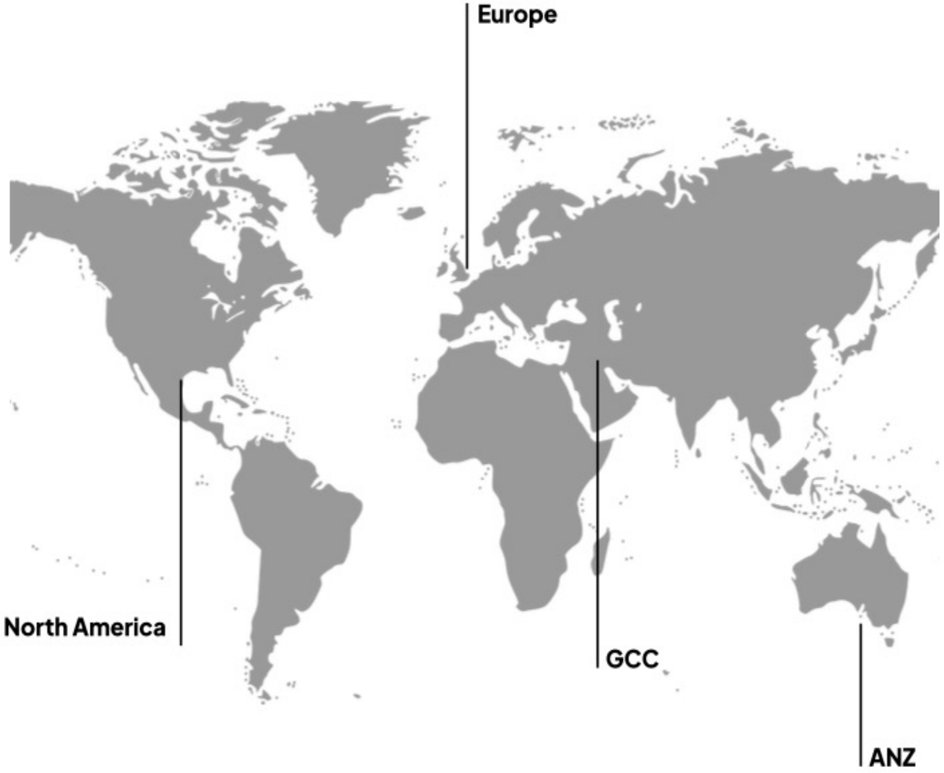
The Threat Discovery Group detects, tracks, and reports on global threats to Industrial Control Systems organizations.

Using a variety of open-source intelligence, proprietary data-sources, and years of threat hunting experience, the Threat Discovery Group enables ICS security teams and stakeholders to take immediate action on threats impacting systems, services, and industries.

Global Coverage

The Threat Discovery Group focuses on threats impacting a variety of key industries in primary regions to support our global customer base.

By using Intelligence Requirements gathered from our customers, and our extensive experience in ICS security, we provide tailored reporting to these customers to ensure they are informed with timely, relevant and actionable intelligence reporting.



Threat Groups

The Threat Discovery Group wouldn't be what it is without uncovering Threat Groups that have specific interests or intent to target the industries we support.

We track over 23 distinct Threat Groups that display the intent or have impacted Industrial Control Systems previously. By understanding what they have done, we can identify what their capabilities are to provide risk-informed recommendations based on your industry and scope.

ELECTRUM

TALONITE

KAMACITE

VANADINITE

XENOTIME

Methodology

TDG satisfies our Intelligence Requirements through a variety of methods. The various methods used in our threat hunts allow us to find threat activity occurring more often than with a single traditional approach. These methods include:

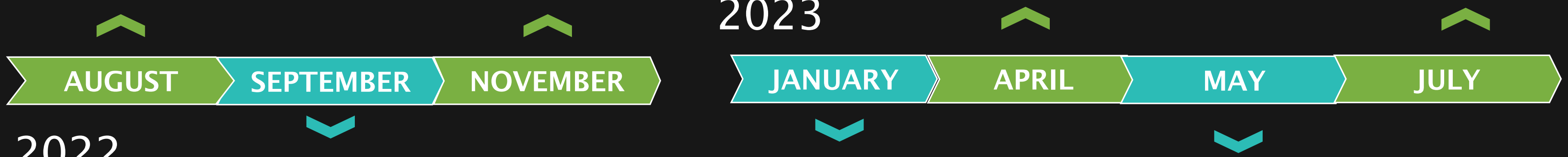
- Hypothesis led, time-bound industry or regional hreat hunts
- Victim-centric threat hunting
- Threat Group-centric threat hunts

Time Bound Threat Hunts

Industry Focused Threat Hunts

Victim Bound Threat Hunts

TRANSPORT & LOGISTICS 2022 – 2023 CYBER EVENTS



AUGUST 2022: Dragos detail low confidence **compromise of Australian transport research and development center.**

SEPTEMBER 2022: **Hacktivist group exploits ride-hailing app** in Russia causing mass traffic congestion.

NOVEMBER 2022: Danish Rail Operator DSB suffers service disruption from **cyber attack against IT subcontractor.**

JANUARY 2023: **CERT-UA detail spear phishing activity against Ukrainian Railways** that Dragos attributes to PETROVITE with low confidence.

APRIL 2023: Alaska Railroad Corp. reports **unauthorized access and data exfiltration** relating to vendors and employees.

MAY 2023: Washington Metropolitan Area Transport Authority detail a January 2023 incident where an **ex-employee's credentials were used for data exfiltration.**

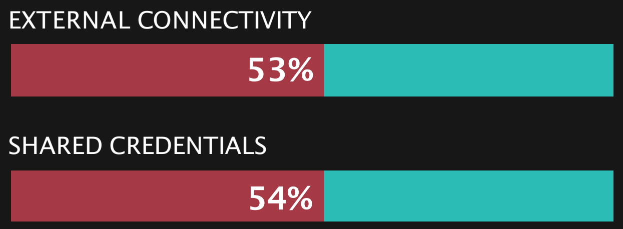
JULY 2023: **Port of Nogoya victim to LockBit 3.0** ransomware.

EXPOSED ICS/OT ASSETS

INTERNET EXPOSED ASSETS & REMOTE ACCESS DEVICES ARE COMMONLY USED FOR INITIAL ACCESS.

Default or weak credentials on ICS/OT devices increases the risk of exposure & compromise.

BASED ON DRAGOS PROFESSIONAL SERVICES ENGAGEMENTS FOR 2022:



Bt

Exploits vulnerabilities in internet-facing assets for espionage, long-term persistence, & interactive operations.

Ko

Compromises internet-exposed remote access devices. Capable of initial access to ICS/OT.

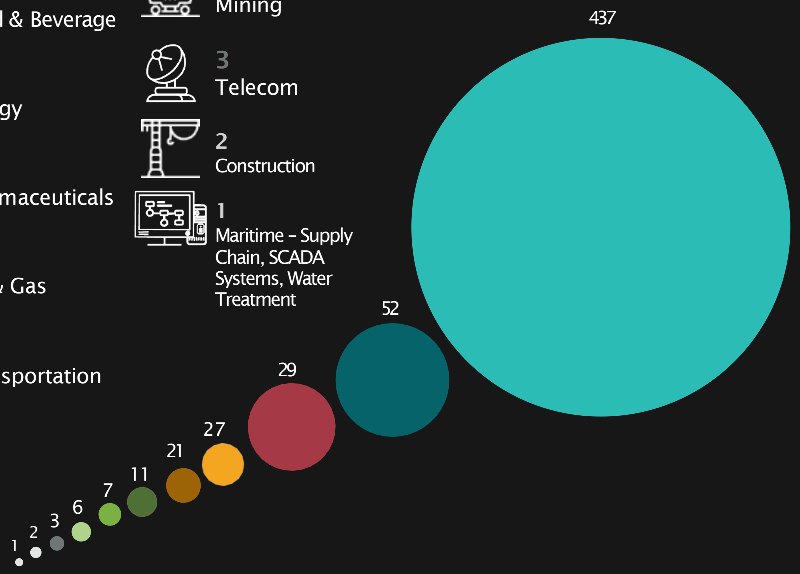
Ka

Exploits vulnerabilities in firewall & router devices. Has facilitated the execution of ICS/OT impact.

RANSOMWARE ATTACKS INCREASED BY 87%

Ransomware Attacks by ICS Sector

437	Manufacturing
52	Food & Beverage
29	Energy
27	Pharmaceuticals
21	Oil & Gas
11	Transportation
7	Engineering, Utilities
6	Mining
3	Telecom
2	Construction
1	Maritime – Supply Chain, SCADA Systems, Water Treatment



October 2022

Data exfiltration of transmission data and Critical Energy/Electric Infrastructure Information (CEII) from a global engineering firm. No known outages.

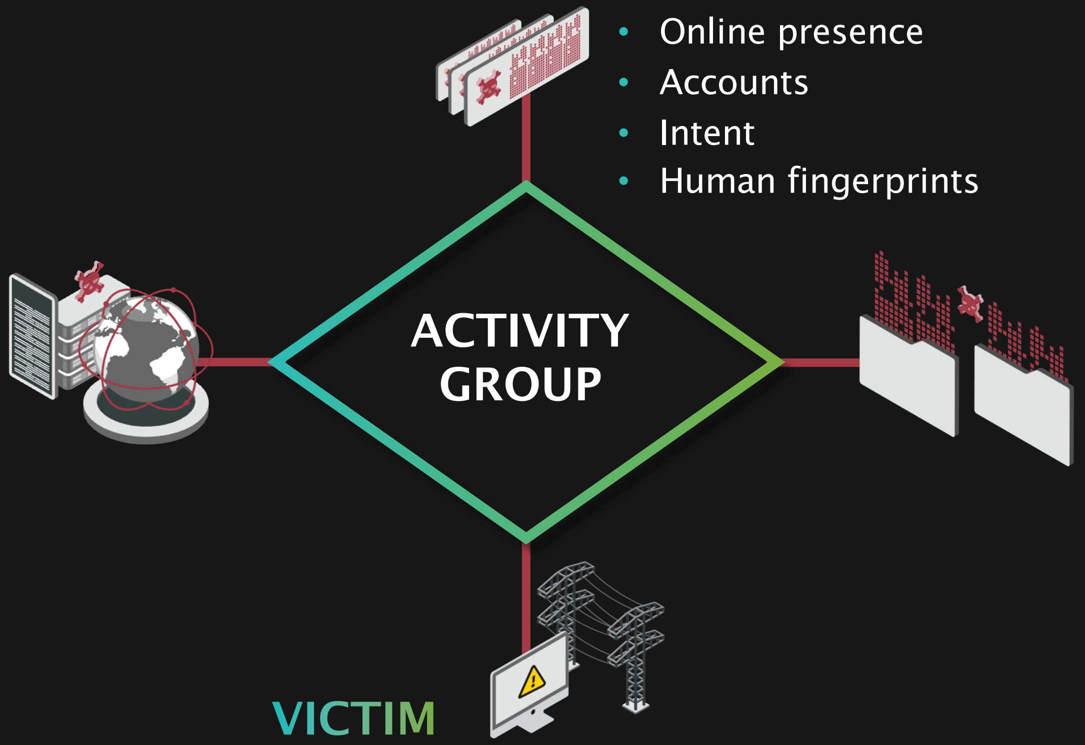
February 2023

During Royal ransomware attack, adversaries likely navigated to ICS/OT environment before detonating ransomware at a US-based energy company.

July 2023

LockBit 3.0 ransomware infection shuts down a Japanese cargo port for multiple days, causing supply chain issues for a major vehicle manufacturer.

The Diamond Model



ADVERSARY

- Online presence
- Accounts
- Intent
- Human fingerprints

INFRASTRUCTURE

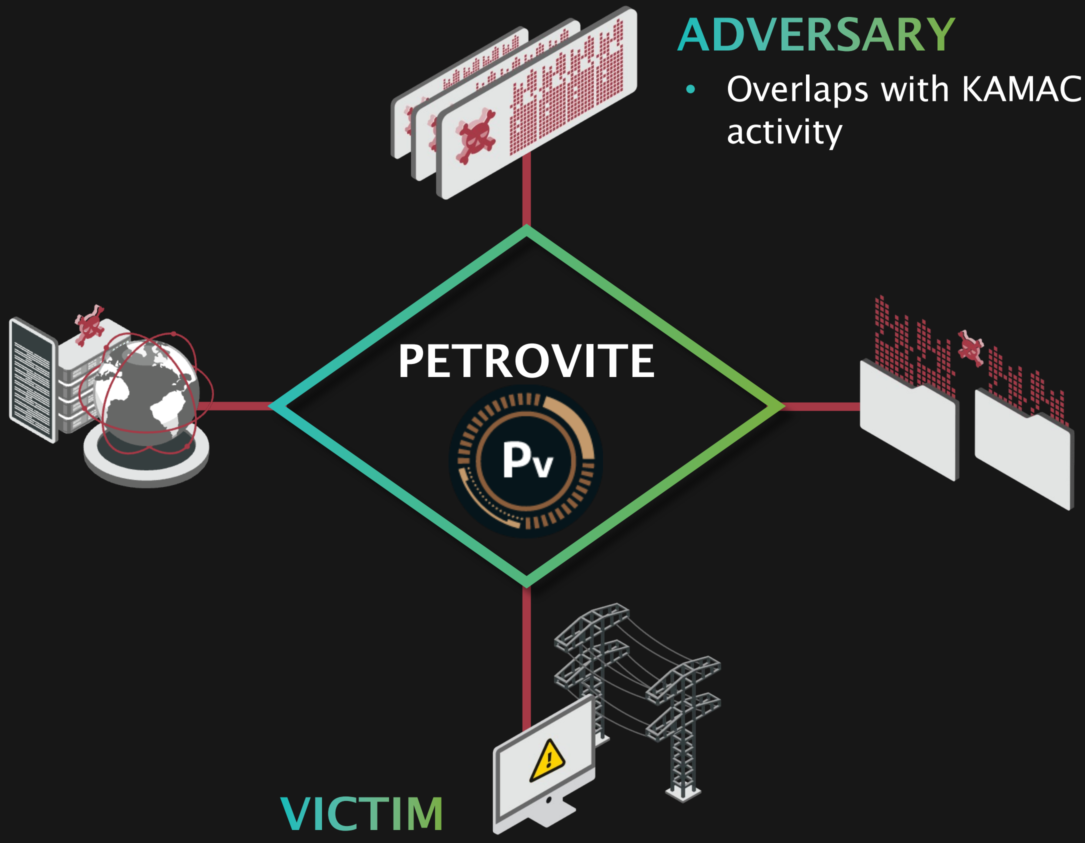
- C2 nodes
- Domains
- Hosting
- Service accounts

CAPABILITIES

- Tools and techniques
- Expertise
- Malware usage: operational, open source, custom
- Exploit development
- Methods of staging data
- Operational discipline

VICTIM

- Recipient of the capabilities:
    - Networks, systems, people, companies
- Apparent target objectives
- At Dragos, a TG is only named if the adversary aims for or purposefully affects ICS and/or OT of its target



PETROVITE

ADVERSARY

- Overlaps with KAMACITE and FANCY BEAR activity

INFRASTRUCTURE

- Legitimate compromised infrastructure
- Tend to be WordPress servers
- Has compromised servers in victim countries
- C2 controller is often a PHP file

CAPABILITIES

- Tailored spear phishing documents
- ZEBROCY – backdoor system reconnaissance and collection capability

VICTIM

- Eurasian Resources Group business units (mining and energy) located in Kazakhstan
- Ukrainian Railways

FIVE CRITICAL CONTROLS

SANS

5 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

01 AN ICS-SPECIFIC INCIDENT RESPONSE PLAN

OT’s incident and response plan is distinct from IT’s.

Different

People	Ops, HES & Maintenance
Consequence	Black start and recovery
Technology	Protocols, systems, logs

Managing the potential impact of an incident is different for OT’s. Create a dedicated plan as well as thought-out next steps for specific scenarios

02 A DEFENSIBLE ARCHITECTURE

The resources and technical skills required to adapt to new vulnerabilities and threats should not be underestimated.

Removing extraneous OT network access points

Mitigating high risk vulnerabilities

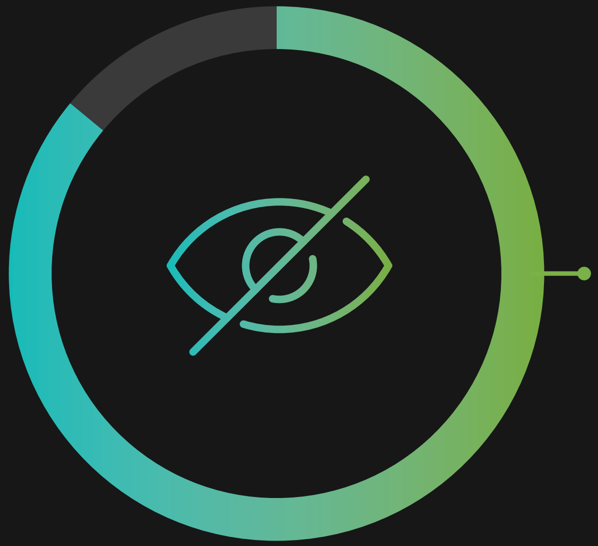
Maintaining strong policy control at IT/OT interface points

The people and processes to maintain it

02 A DEFENSIBLE ARCHITECTURE

03 OT VISIBILITY

You can't protect
what you can't see.



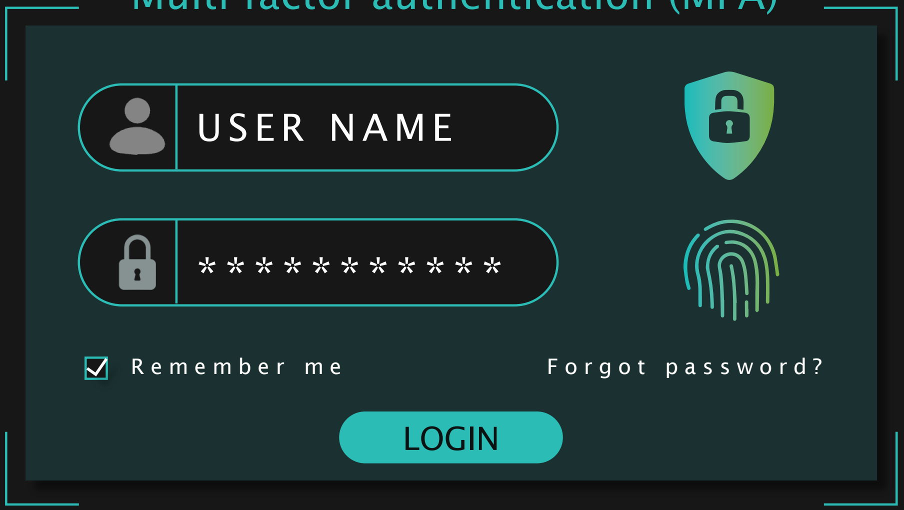
IN 2021
86%
of Dragos services customers had limited to no visibility in their OT environments

A Successful
OT Security Posture

- Maintains an inventory of assets
- Maps vulnerabilities against those assets
- Actively monitors traffic for potential threats
- Validates the security controls implemented in a defensible architecture

04 Secure Remote Access

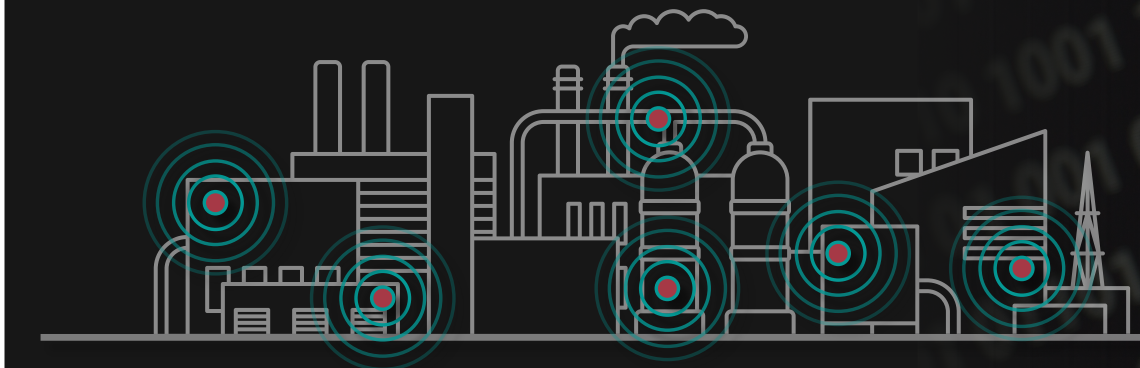
Multi-factor authentication (MFA)



MFA is a rare case of a classic IT control that can be appropriately applied to OT.

Implement MFA across your systems of systems to add an extra layer of security for a relatively small investment.

05 KEY VULNERABILITY MANAGEMENT PROGRAM



Knowing your vulnerabilities
and having a plan to manage them is a critical component to a defensible architecture.

DRAGOS OT-CERT*

Industrial cybersecurity resources for the OT community

FREE CYBERSECURITY RESOURCES

Free content available for OT asset owners and operators, to help you build and maintain an effective OT cybersecurity program

OPEN TO GLOBAL ICS/OT COMMUNITY

Oriented toward Small and Medium Businesses (SMBs) and resource-challenged organizations with OT environments that lack in-house expertise

NEW CONTENT MONTHLY

Members have access to a growing library of resources such as reports, webinars, training, best practice blogs, assessment toolkits, tabletop exercises and more, available from the OT-CERT portal

REGIONAL WORKSHOPS

Customized regional workshops to meet the needs of the community

VULNERABILITY DISCLOSURES

We take a coordinated approach to the disclosure of vulnerabilities, working with vendors to better protect our customers and the ICS/OT community

*Operational Technology –
Cyber Emergency Readiness Team

OT-CERT Resources available now

OT Cybersecurity Fundamentals Self-Assessment

Asset Management Toolkit
Collection Management Framework Toolkit
Host-Based Logging Toolkits
Incident Response Plan Toolkit
OT Backups Toolkit
Secure Remote Access Toolkit

Best Practices Blog Series

Self-Service OT Ransomware Tabletop Toolkit

ICS/OT Cybersecurity Introductory Training, Guides, and Videos

Joint Workshops with Partners

OT-CERT Working Sessions
Tips & Tricks from Members

ICS/OT Vulnerability Disclosures
Victim Notifications

DRAGOS

Your opportunity to get technical, in-depth research findings and insights from Dragos experts and ICS/OT practitioners on the front lines

DISC 2023

DRAGOS INDUSTRIAL SECURITY CONFERENCE AUSTRALIA

Thursday, 30 November 2023
Melbourne

Register your interest at:
https://hub.dragos.com/anz-disc-2023