Middle East Escalation

What the Current Threat Landscape Means for APAC OT Environments

DRAGOS

Mike Hoffman

Field CTO, Oil & Gas and Petrochemicals

linkedin.com/in/mjhoffman7

- 26 years of experience across automation and ICS/OT security, with roles in O&G downstream, upstream, and global technical leadership
- Past titles have included Principal Consultant, Principal ICS Security Engineer, Controls & Automation Specialist, Process/CEMS Analyzer Specialist, and Instrumentation & Electrical Technician
- Certified SANS Instructor ICS410/ICS612, GSE #320, Master's in Information Security Engineering from SANS Technology Institute

Background

Kinetic Attacks begin in Iran on Feb 28, 2026

How cyber was used during the operations

Retaliation attacks

Middle East Developments

Kinetic Attacks

- Qatar LNG assets have been impacted and have declared Force Majeure. Over 17% reduction in global LNG output
- Bahrain Refinery production was affected due to a drone strike, and has declared Force Majeure
- Kuwait Refineries are at reduced capacity and have declared Force Majeure
- Saudi Arabia's refineries targeted
- UAE Refineries, Gas Fields, and Oil Terminals targeted
- Oman Oil Terminas targeted
- Strait of Hormuz shipping lane effectively blocked – affecting 20% of global oil supply and significantly disrupting LNG and chemicals exports

Middle East Developments

Cyber Attacks

- Considerable amount of GPS attacks around the Strait of Hormuz
- Reported Adversarial activity and data exfiltration in LNG companies
- BAUXITE claimed Jordanian wheat silo compromise
- MuddyWater increased activity against the US. Israel (historically targeting the EU, but it's shifting focus to the US, Israel, and allied countries)
- Hacktivism is on the rise (claims have doubled since the start of the war)

ICS CYBER KILL CHAIN

Initial survey & access to the enterprise IT environment

STAGE 1

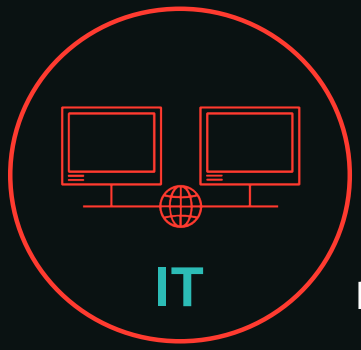
Crossing into ICS/OT

STAGE 2

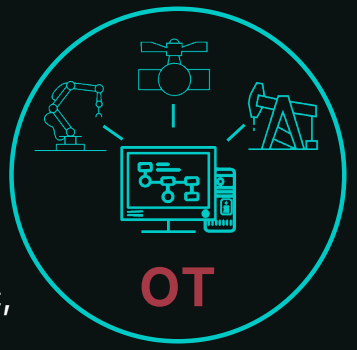
OT network reconnaissance, penetration, & execution of ICS attacks

Avoid Custom Software & Malware

Emphasize Commodity & System Tools



Different systems, network traffic, adversaries, & need to manage vulnerabilities differently



Custom Attack Packages Tailored to a Specific Environment

Limited Ability to Replay or Reuse Attacks

DRAGOS

BAUXITE

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

2023

Bx

- 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:

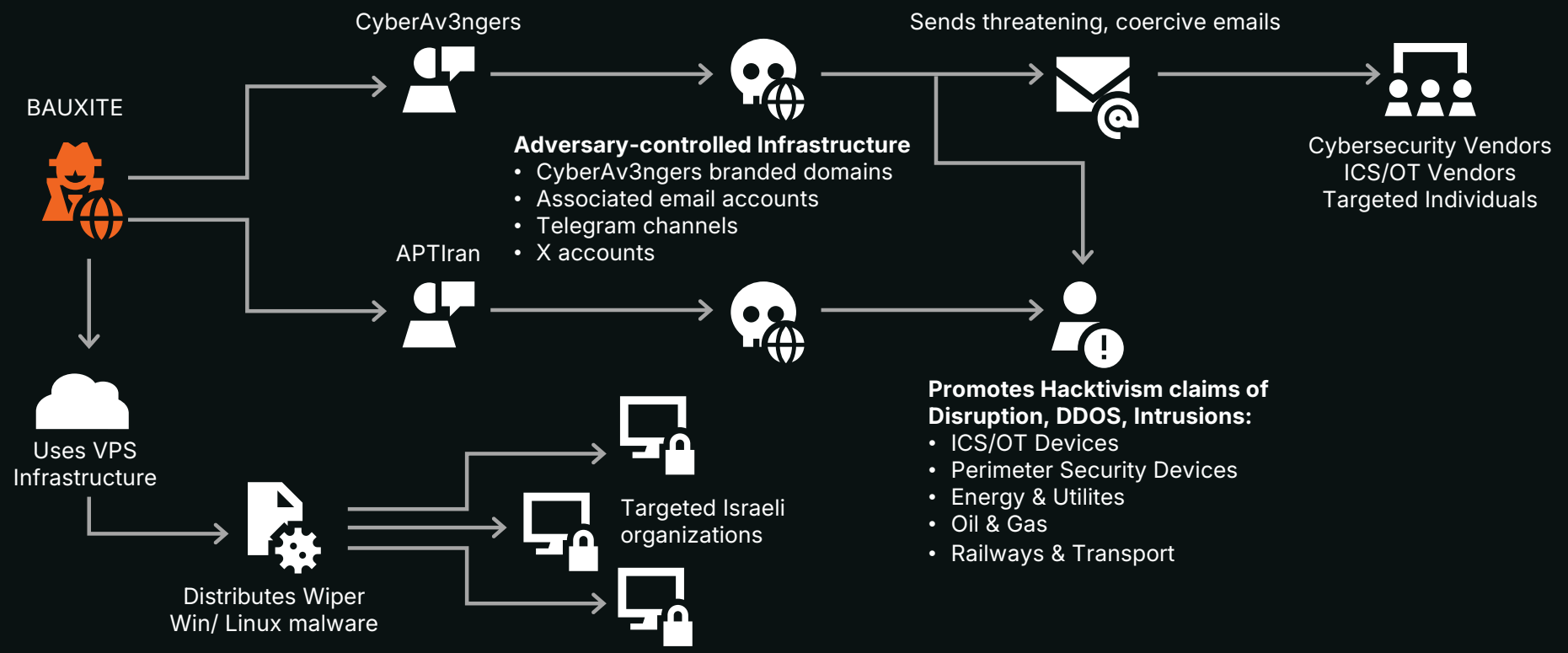
Critical infrastructure globally, with focus on organizations with internet-exposed OT devices

Overlaps with: CyberAv3ngers (hacktivist persona)

BAUXITE Activity

01 Psychological, Influence Operations

02 Destructive attacks against Israeli targets



TAT25-78 (MuddyWater)

RMM tool abuse and intelligence-driven access operations targeting ICS-adjacent environments

- Abused legitimate RMM tools (Atera and others) to establish persistent IT access
- Targeted industrial supply chains and enterprise networks supporting ICS operations
- Significant activity increase since January 2026, with new access pathways under development
- Reported increased scanning of logistics and energy organizations in the United States and Australia throughout February 2026

Targets: Government, defense, and critical infrastructure sectors

Overlaps with: MuddyWater

PYROXENE

Cross-domain access enabling movement from IT into OT networks

SINCE 2025

Py

- 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)

PYROXENE Attack Path

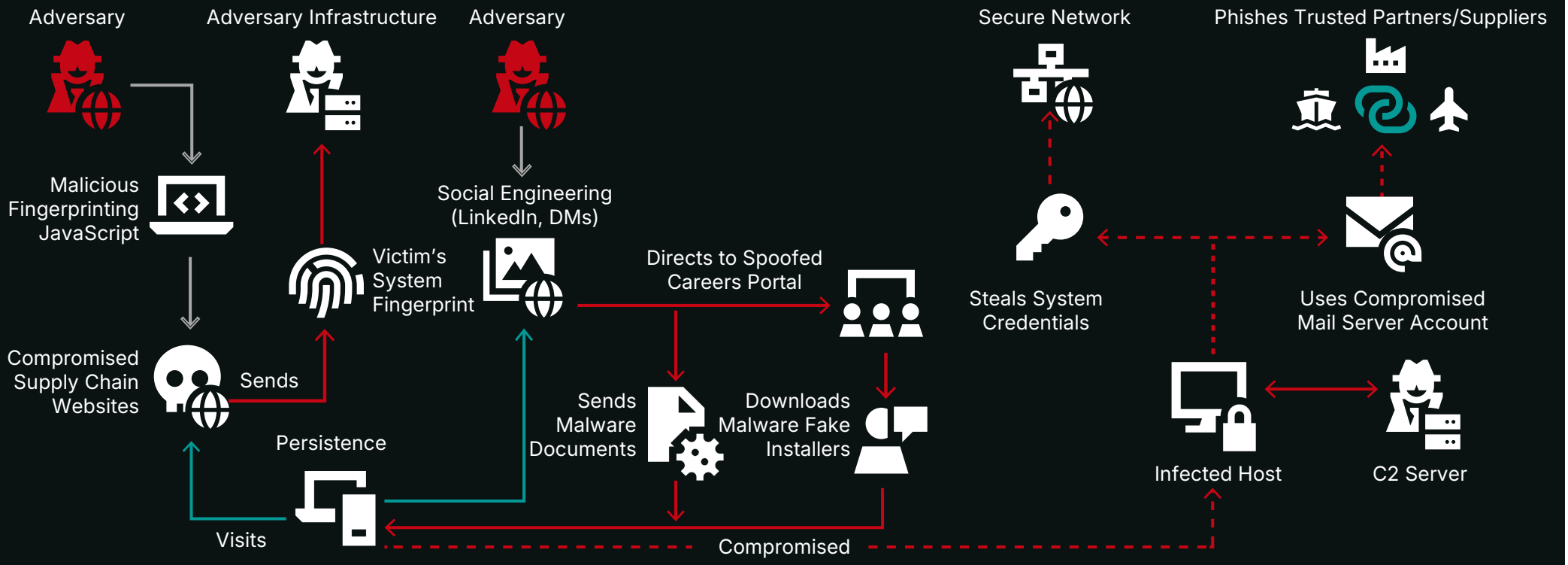
01 Strategic website compromises

02 Social engineering campaign

03 Deploy RAT/Backdoor Infect Victim Host

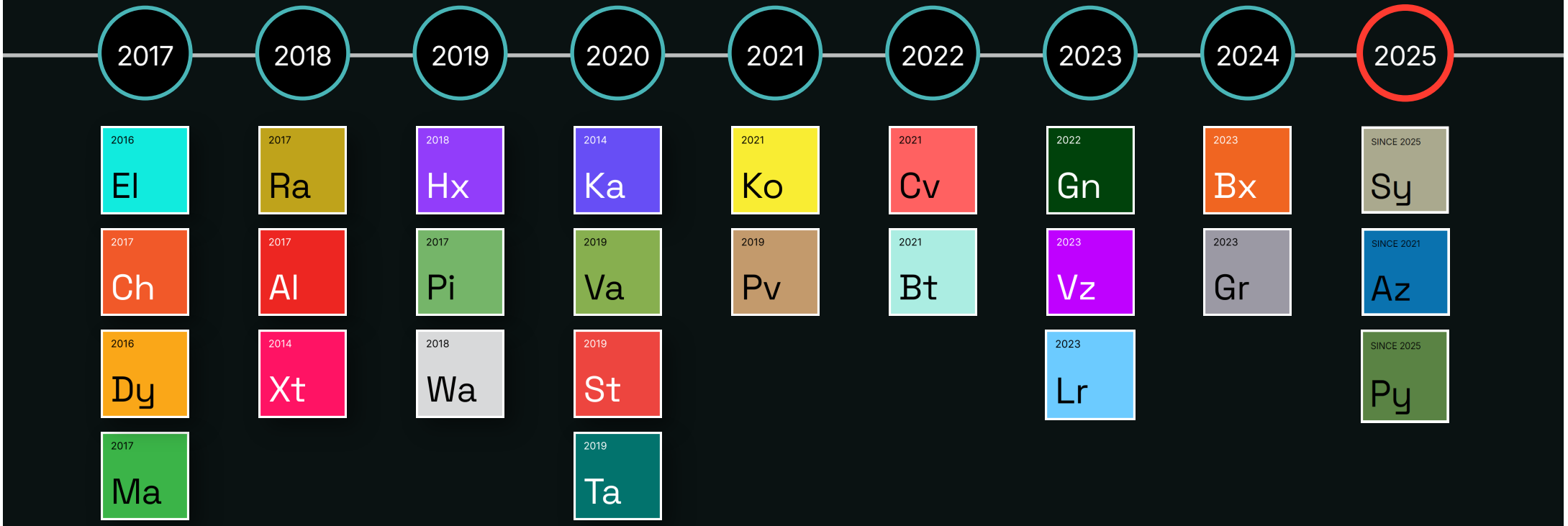
04 Lateral movement into secure network

05 Supply Chain Attack



Dragos Tracked Threat Groups

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



PARISITE

Initial access facilitation targeting ICS/OT-adjacent environments across critical infrastructure

2017

Pi

- Exploited N-day VPN & remote service vulnerabilities
- Operated Pay2Key RaaS
- Sold compromised credentials via Initial Access Brokers
- Used profile to promote disruptive cyber activity

Targets:

Electric | Oil & Gas | Manufacturing | Transportation | Defense | Government

Overlaps with: Fox Kitten, Lemon Sandstorm

PARISITE – INITIAL ACCESS BROKER

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)

PYROXENE – AVIATION, MARITIME, DEFENSE

MAGNALLIUM

Credential theft, wiper attacks, and espionage operations targeting critical infrastructure

SINCE 2013

Ma

- Espionage operations focused on long-term intelligence collection against defense, infrastructure, and government targets
- Custom wiper malware (StoneDrill, ZeroCleare, Dustman) and backdoors (POWERTON, Tickler) deployed alongside LOTL techniques
- Credential theft and abuse of exposed access points to establish ICS/OT-adjacent footholds

Targets:

Targeting OT in US, Europe, Middle East, South Korea, and Australia

Overlaps with: APT33, Refined Kitten

MAGNALLIUM – COMMUNICATIONS/SATELLITE

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

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

01 ICS Incident Response Plan

- Assume enterprise disruption will affect operations, even without direct OT system interaction
- Ensure you have offline, tested backups for EWS, historians, SCADA servers, and hypervisors
- Focused on loss of availability, control, and/or view, unauthorized PLC logic changes, OT asset defacement, and unexpected controller state changes, support rapid identification of the intrusion root cause
- Persistence-oriented IR workflows
- Coordination among OT, IT, and executive leadership during incidents involving public claims or influence activity

02 Defensible Architecture

- Eliminate internet exposure for OT devices, controllers, and management interfaces
- Harden edge devices and identity gateways
- Validate segmentation boundaries, ensure IT → OT pathways are minimized and monitored
- Lock down remote services (RDP, VNC, SSH, vendor portals)
- Restrict access to management interfaces and DMZ devices

03 ICS Network Monitoring Visibility

- Monitor OT and IT environments for anomalous use of legitimate administrative tools
- Detect unauthorized OT interactions – unusual write operations, PLC logic upload/download, firmware/config changes, atypical external communications originating from OT environments, and abnormal data movement
- Detect tunneling/proxy patterns originating in or traversing OT zones
- Alert on first-seen outbound destinations from OT segments — new domains/IPs, unknown TLS certificates/fingerprints, and sudden egress to cloud providers
- Perform proactive threat hunts adversarial behaviors and TTPs

04 Secure Remote Access

- Inventory every remote access pathway – internal, vendor, cloud
- Enforce strong remote access controls, including timely patching of internet-facing services, MFA across all remote access pathways, and strict governance of VPN and third-party access
- Ensure that access is time-bound and monitored
- Route access through monitored jump hosts
- Remove default/shared credentials
- Disable remote management interfaces unless needed, only allow-list trusted IPs

05 Risk-Based Vulnerability Management

- Prioritize vulnerabilities in VPNs, firewalls, exposed OT services, and identity systems
- Harden or remove misconfigurations enabling unauthenticated access
- Apply compensating controls when patching isn’t feasible
- Track vulnerabilities in OT-adjacent IT systems

Call to Action

Send your queries to: ME_APAC_Queries@dragos.com

DRAGOS

2026 OT/ICS Cybersecurity Report: A Year in Review

Strengthen your industrial defenses with the latest threat intel and strategic recommendations.

EXPLORE THE INSIGHTS →