Middle East Escalation

Assessing Spillover Threats to OT/ICS

Melissa Messare

Senior Threat Intel Analyst, Dragos

DRAGOS

Background

Kinetic Attacks begin in Iran on Feb 28, 2026

How cyber was used during the operations

Retaliation attacks

Activity Since Feb 28

BAUXITE

Attack on a Jordanian wheat silo

TAT25-78 (MuddyWater)

Increased, indiscriminate activity against the U.S. and Israel

Hacktivism

Key patterns typically seen during a geopolitical crisis

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)

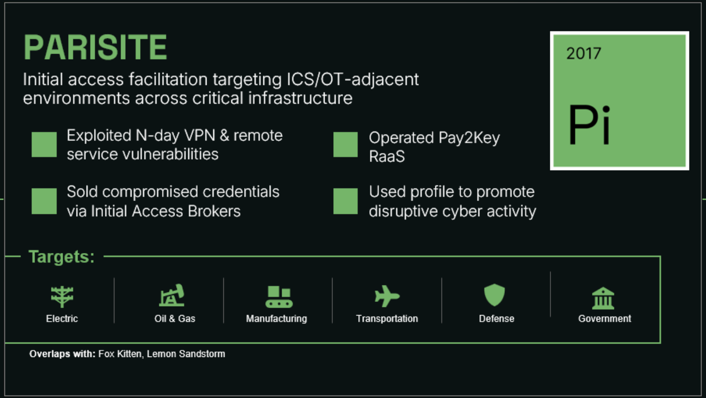
TAT25-78 (MuddyWater)

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

Targets: Government, defense, and critical infrastructure sectors

Overlaps with: MuddyWater



PARISITE

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

2017

Pi

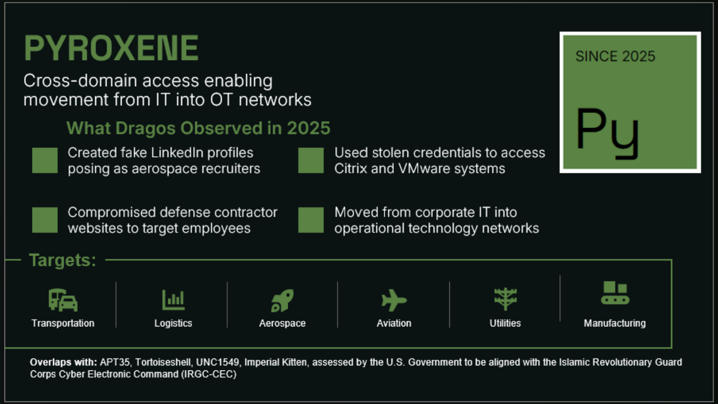
- Exploited N-day VPN & remote service vulnerabilities
- Operated Pay2Key RaaS
- Sold compromised credentials via Initial Access Brokers
- Used profile to promote disruptive cyber activity

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

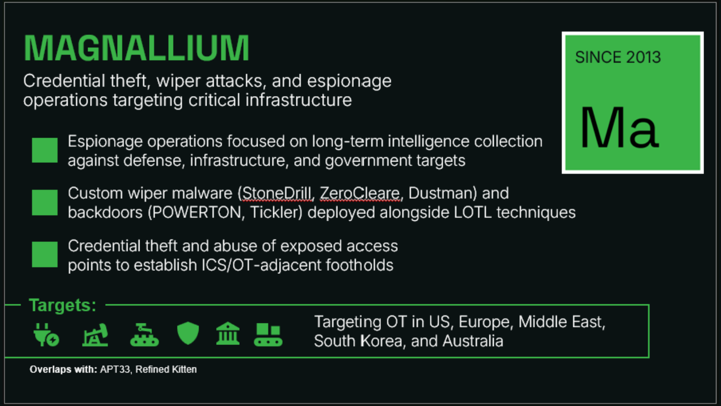
- Created fake LinkedIn profiles posing as aerospace recruiters
- Used stolen credentials to access Citrix and VMware systems
- Compromised defense contractor websites to target employees
- Moved from corporate IT into operational technology networks

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

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 controller interaction
- Prepare for manual operations – 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
- Detail roles for IT security, OT engineering, SCADA operators, and operations leadership

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
- Baseline OT communications and alert on deviations
- 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

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
- 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

Key Take Aways for Defenders

- **Expect Stage 1 Activity**
    - Primary Operational Risk
- **Adversaries Will Target Exposed ICS/OT Assets**
    - Eliminate or lock down internet-facing devices
- **Prepare for Manual Operations**
    - Ensure you have offline tested backups
- **Expect & Accept Hacktivist Noise**
    - DDoS campaigns, exaggerated claims of operational disruption

Q&A

QUESTIONS AND ANSWERS

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 →

DRAGOS

9TH ANNUAL | 2026

YEAR IN REVIEW

OT/ICS CYBERSECURITY REPORT