Presented by Trellix ADVANCED RESEARCH CENTER

OPERATIONAL TECHNOLOGY THREAT REPORT

November 2025

EXECUTIVE SUMMARY

From April 1 to September 30, 2025, operational technology (OT) and industrial control systems (ICS) faced unprecedented threats from sophisticated adversaries. Trellix telemetry detected **272,512 OT/ICS-related threats** across **572 unique customers**, while **333 ransomware attacks** specifically targeted critical infrastructure sectors.

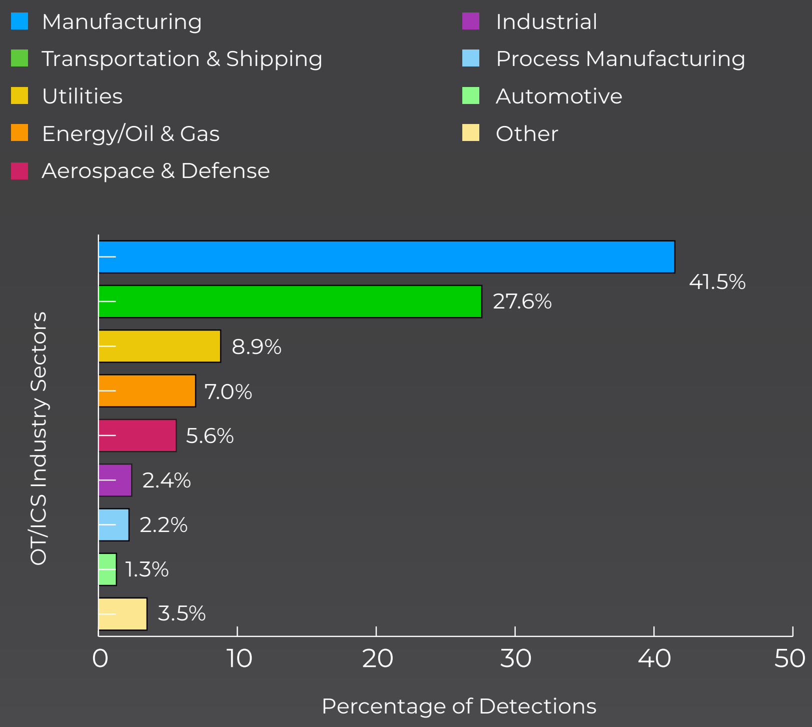
The threat landscape reveals coordinated campaigns by state-sponsored actors and ransomware groups, with the manufacturing, transportation and shipping, utilities, and energy/oil and gas sectors bearing the highest risk. Notable threat actors include Sandworm Team, Qilin ransomware, and specialized groups like TEMP.Veles targeting safety systems.

OT THREAT LANDSCAPE OVERVIEW

The global OT threat environment has intensified significantly, driven by geopolitical tensions and the increasing digitization of industrial systems. State-sponsored actors from Russia, Iran, and North Korea have expanded their targeting of critical infrastructure, while ransomware groups have developed specialized capabilities for OT environments.

Manufacturing emerged as the primary target, representing 41.5% of all detections. This concentration reflects the sector's critical role in global supply chains and often inadequate OT security measures. Transportation and shipping ranked second in detections with 27.6%, and the utilities, energy/oil and gas, and aerospace and defense industries accounted for a combined 21.5% of detections.

PRIMARY OT/ICS INDUSTRY TARGETS (APRIL 1–SEPTEMBER 30, 2025)



This breakdown represents threats detected primarily within IT infrastructure of organizations operating in OT/ICS industries, rather than detections from OT environments themselves. These detections across email (55.6%), network perimeter (25.4%), and endpoint (18.5%) environments provide critical visibility into threats targeting industrial sectors, as IT compromise often serves as the primary entry point for attacks that can impact connected OT systems.

Geopolitical factors significantly influenced targeting patterns. Russian-linked groups focused on Ukrainian energy infrastructure, while Iranian actors concentrated on regional petrochemical facilities. The ongoing conflict in Ukraine has accelerated the weaponization of cyber capabilities against industrial systems.

THREAT ACTOR ACTIVITY

Sandworm Team (Russia, GRU Unit 74455)

Profile

Sandworm Team, also known as BlackEnergy, Voodoo Bear, or Iron Viking, remains one of the most aggressive and capable state-sponsored threat actors targeting OT environments. Operated by Russia's GRU Main Center for Special Technologies (GTsST, Unit 74455), Sandworm has specialized in cyber-physical disruption as part of Russia's hybrid warfare strategy.

Activity and Tactics

Between 2022 and 2025, Sandworm dominated industrial threat telemetry, responsible for nearly a third of observed OT-related intrusions. They continued systematic campaigns against Ukrainian energy, telecommunications, and government networks, deploying Industroyer2 to disrupt power substations, and multiple destructive wipers—CaddyWiper, NikoWiper, and ORCSHRED—to erase system data and impede restoration efforts. Their operations often coincide with kinetic military actions, suggesting coordination between cyber and conventional warfare.

Impact and Outlook

Sandworm's campaigns have demonstrated a repeatable, modular attack model for targeting ICSes, positioning them as the benchmark for nation-state-level OT threats. The group's persistent evolution of wiper families and exploitation of both IT and OT protocols indicates ongoing R&D investment. Their activity reinforces the need for resilience-based defense, rapid system restoration, offline backups, and out-of-band communication in conflict-prone regions.

TEMP.Veles / XENOTIME (Russia-linked, Safety Systems Focus)

Profile

TEMP.Veles, also tracked as XENOTIME, is an elite, possibly Russian-linked actor behind the TRITON (also known as TRISIS or HatMan) malware. They specialize in compromising **safety instrumented systems (SIS)**, specifically the Triconex controllers used to prevent catastrophic failures in industrial plants.

Activity and Tactics

Their hallmark intrusion, against a **Saudi Arabian petrochemical facility in 2017**, aimed to reprogram safety controllers to cause physical damage or loss of life. Since then, TEMP.Veles has been observed conducting reconnaissance and persistence operations in energy and chemical facilities worldwide. They exploit engineering workstations and system integrators' credentials to move laterally into OT environments. Their operations involve **multistage intrusions blending IT exploitation with OT protocol manipulation**, demonstrating deep process understanding.

Impact and Outlook

TEMP.Veles/XENOTIME remains the **most technically advanced OT adversary known**, being the only actor to directly attempt to subvert safety systems. Their ongoing reconnaissance activity suggests intent to maintain contingency access for potential future sabotage. For defenders, this group underscores the importance of **monitoring safety networks separately**, auditing SIS firmware integrity, and isolating engineering workstations with strict change control.

Qilin Ransomware Group (Cybercriminal, OT-targeting Affiliate Network)

Profile

Qilin (also known as Agenda) represents the new generation of ransomware-as-a-service (RaaS) operations explicitly extending into industrial environments. While financially motivated, their operations increasingly exhibit knowledge of industrial dependencies, particularly in energy distribution and water treatment sectors.

Activity and Tactics

From mid-2024 through 2025, Qilin led all ransomware activity against industrial entities, with 63 confirmed attacks, including against Uganda Electricity Transmission Company and several water utilities across Europe and Asia. They often deploy dual-use payloads capable of disrupting both IT and OT networks by encrypting shared engineering resources, configuration servers, and historian systems. Qilin's use of Agenda ransomware variants with Windows and Linux payloads allows cross-platform execution within mixed environments. Recently Qilin has claimed responsibility for the attack against the Asahi brewery in Japan.

Impact and Outlook

Qilin exemplifies the blurring of criminal and OT-focused threats, leveraging ransomware as both extortion and disruption tools. Their success underscores how ransomware operators are learning to exploit availability-sensitive environments for maximum leverage. Continued cross-sector collaboration and shared telemetry between IT SOCs and OT defenders are essential to counter their expanding reach.

APT33 and APT34 (Iran, Oil and Gas Espionage and Sabotage)

Profile

APT33 (Elfin) and APT34 (OilRig) are Iranian state-linked groups active since the mid-2010s, both heavily focused on the energy sector and regional rivals in the Gulf. Initially known for cyber espionage and credential harvesting, both groups have gradually adopted destructive components in their operations.

Activity and Tactics

APT33 has targeted aviation, petrochemical, and manufacturing networks to exfiltrate intellectual property and credentials for follow-on access. APT34 maintains persistent footholds in energy and government environments through phishing and exploitation of web-facing infrastructure. In later campaigns, both groups deployed Shamoon and ZeroCleare wipers to cause data loss and downtime. Their tooling suggests increasing maturity and partial convergence in tradecraft, with shared infrastructure and overlapping objectives. More details on the Iranian cyber capabilities can be found in our public research.

Impact and Outlook

Iranian operations have evolved from opportunistic espionage to strategic cyber coercion, often timed with geopolitical tensions. The dual-use nature of their campaigns—espionage followed by destruction—makes them particularly challenging to defend against. Enhanced identity management, network segmentation, and endpoint telemetry in OT DMZs remain critical mitigation layers for organizations in the energy sector.

Recent Campaigns (2025 Focus)

- **PathWiper (Ukraine, June 2025):** A destructive campaign targeting Ukrainian energy operators, possibly linked to Sandworm, designed to mimic ransomware while permanently erasing data. It reinforces Russia's continued use of pseudo-ransomware to mask politically motivated sabotage.
- **Blue Locker (Pakistan, 2025):** Ransomware incidents affecting Pakistan's oil and gas companies. The operators blended criminal and geopolitical motives, leveraging access through local vendors and exposing the fragility of third-party OT service ecosystems.
- **Static Tundra (Global, 2025):** A campaign exploiting unpatched Cisco IOS vulnerabilities to gain access to telecommunications and manufacturing networks. Believed to be an advanced persistent actor using compromised network equipment as staging points for lateral movement into OT segments.

Strategic Context

From 2020 to 2025, the OT threat landscape shifted from isolated, state-linked disruptions to a converged ecosystem of state and criminal actors with overlapping methods and targets. State groups such as Sandworm Team and TEMP.Veles pursue strategic disruption, while hybrid and ransomware groups like Qilin exploit the same pathways for profit. The recurring themes—compromised remote access, supply chain abuse, and destructive malware disguised as ransomware—highlight the urgency of integrating threat intelligence, OT network visibility, and supplier accountability into critical infrastructure defense models.

TACTICS, TECHNIQUES, PROCEDURES (TTPS)

The most prevalent attack techniques target the IT-to-OT boundary, exploiting insufficient network segmentation. PowerShell emerged as the primary attack vector (96,061 detections), followed by Cobalt Strike (85,986 detections) for post-exploitation activities.

MITRE ATT&CK for ICS Mapping

- **T1046 – Network Service Scanning:** Industrial protocol discovery
- **T1021.002 – SMB/Windows Admin Shares:** Lateral movement to engineering workstations
- **T1078 – Valid Accounts:** Compromised engineering credentials
- **T1485 – Data Destruction:** Process data and safety system targeting
- **T1489 –Service Stop:** Safety system manipulation

IT-to-OT pivoting occurs through compromised engineering workstations, shared credentials, and exploitation of remote-access solutions. Attackers leverage legitimate industrial protocols (Modbus, DNP3, IEC 61850) to blend malicious commands with normal operations, making detection challenging.

Advanced groups deploy specialized tools like **Industroyer** for direct control of electricity substation switches and **TRITON** for safety system manipulation. These capabilities represent a significant escalation from traditional IT-focused attacks to operations capable of causing physical damage.

VULNERABILITY AND EXPOSURE INSIGHTS

Legacy industrial protocols remain the primary attack surface, with Modbus, DNP3, and proprietary SCADA protocols lacking inherent security features. Human-machine interfaces (HMIs) and engineering workstations frequently serve as pivot points due to dual IT/OT network connectivity. To frame the operational hierarchy, this report references the ISA-95/Purdue Model, where Level 4/3 encompasses Enterprise and Manufacturing Operations Management (MES) systems, Level 2 includes Supervisory Control (HMIs and SCADA), and Level 1/0 covers the physical controllers and sensors (PLCs).

Programmable logic controllers (PLCs) face increasing targeting, particularly Schneider Electric Triconex systems (TRITON attacks) and Siemens controllers. Remote-access solutions, including VPNs and remote desktop protocols, provide initial access vectors when improperly secured.

Vendor response times vary significantly, with critical OT vulnerabilities often requiring extended patching cycles due to operational constraints. The average time from vulnerability disclosure to patch deployment in OT environments exceeds 180 days, compared to 30 days for traditional IT systems.

The most significant trend defining the current OT threat landscape is the strategic focus on the IT/OT boundary. Threat actors, recognizing the inherent difficulties and high visibility risks of directly targeting low-level controllers, are instead prioritizing the compromise of Level 3 and Level 4 systems that bridge the networks.

These boundary devices and industrial software platforms offer an easier and more scalable entry point through common IT-like vulnerabilities (such as RCE in remote-access tools and enterprise applications) but yield highly kinetic OT outcomes—namely, the ability to manipulate production data, disable safety controls, or force widespread disruption across the control plane. This dynamic means that perimeter defense is now more critical than ever for maintaining operational integrity.

The specific CVE examples detailed below are intended not as an exhaustive list, but rather as representative cases of the high-impact vulnerabilities disclosed and actively exploited during the Q2 and Q3 2025 period. These instances collectively illustrate the shifting focus of modern threat actors toward strategic pivot points within the industrial ecosystem.

1. Exploitation in Perimeter and Remote-access Devices

Critical network infrastructure devices—which are frequently used to segment or provide remote access into OT networks—were under constant attack. Exploiting these flaws provides unauthenticated, root-level access to the internal network.

- **Cisco ASA/FTD Zero-Day Campaign (CVE-2025-20333 & CVE-2025-20362):** A state-sponsored threat actor, linked to the “ArcaneDoor” activity, actively exploited a chain of zero-day vulnerabilities in Cisco ASA and Firepower Threat Defense (FTD) devices in Q3 2025. This campaign provided unauthenticated access and remote code execution (RCE) on the firewalls themselves, with attackers even modifying the devices’ firmware (ROMMON) for persistence across reboots.

  OT Risk Connection: These devices form the network boundary; compromising them means the primary segmentation defense is completely nullified, granting the attacker unfettered access to OT network segments for lateral movement and reconnaissance. This translates directly to loss of network defense.

- **Erlang/OTP SSH RCE (CVE-2025-32433):** This flaw (CVSS 10.0) in the Erlang SSH library—found in many networking components and OT appliances—allowed an unauthenticated remote attacker to execute code. Exploitation attempts were observed in Q2 2025 targeting exposed ports.

  OT Risk Connection: Many hardened Linux-based control servers, data historians, and communication gateways in OT environments rely on Erlang/OTP for management interfaces. An unauthenticated RCE on these systems provides a high-privilege foothold inside the control network, leading to potential loss of view (tampering with historian data) or an immediate pivot point.

2. Compromise of IT-integrated Industrial Software

Vulnerabilities in software that links business systems (ERP) to manufacturing processes (MES) serve as high-privilege pivot points into the core OT environment.

- **SAP NetWeaver RCE Chain (CVE-2025-31324 & CVE-2025-42999):** This pair of critical vulnerabilities in SAP NetWeaver's Visual Composer was actively exploited by multiple ransomware and espionage groups (including Qilin and BianLian) throughout Q2 2025.

  OT Risk Connection: SAP NetWeaver is the primary source for production scheduling, bill of materials (BOM), and quality control data fed directly into manufacturing execution systems (MES). Compromising this platform allows actors to subtly poison or disrupt the core production data, potentially causing batch errors, quality failures, or unexpected operational halts (loss of integrity and control).

- **Dassault DELMIA Apriso RCE (CVE-2025-5086):** This critical RCE flaw in the DELMIA Apriso Manufacturing Operations Management (MOM) software was added to the CISA KEV catalog in Q3 2025 due to confirmed exploitation in the wild.

  OT Risk Connection: As an MES/MOM platform, Apriso orchestrates the entire factory floor, tracking assets, labor, and process flow. RCE on this server means an attacker gains control over the system that drives the industrial workflow, leading to loss of visibility (spoofing production reports) and the potential to issue malicious commands to control systems (loss of control).

3. High-risk Direct OT Device Disclosures

These critical flaws target the controllers themselves, representing the inherent risk in vendor product lines and the long-term threat of unpatchable OT infrastructure.

- **Rockwell ControlLogix RCE (CVE-2025-7353):** A critical vulnerability in ControlLogix Ethernet modules allows an unauthenticated attacker to gain RCE by leveraging an unintended web-based debugger endpoint.

  OT Risk Connection: The Ethernet module is the communications spine of the PLC chassis. Gaining RCE here means an attacker can tamper with or halt communications to the processor, facilitating the injection of malicious logic or disabling safety functionality without the need for engineering credentials.

- **Rockwell DoS Flaws (CVE-2025-24478 & CVE-2025-9166):** Multiple high-severity flaws that allow an unauthenticated, remote attacker to trigger a major non-recoverable fault (MNRF) or a denial of service (DoS) condition on GuardLogix and ControlLogix PLCs.

  OT Risk Connection: This directly compromises availability, forcing the controller into a failed state that requires a physical power cycle to resolve. In continuous process environments, this leads to immediate, unscheduled production shutdown, material spoilage, and significant economic impact.

- **ABB ASPECT Authentication Bypass (CVE-2025-53187):** A critical (CVSS 9.8) flaw in ABB ASPECT systems that permits an unauthenticated attacker to bypass security and gain administrative control.

  OT Risk Connection: ASPECT is a building management system (BMS) or control management system (CMS). Compromise grants control over physical facility infrastructure (HVAC, ventilation, power management). This control can be leveraged for safety risk (e.g., manipulating air pressure in a clean room) or to facilitate physical intrusion by unlocking access controls.

Key Takeaways

- **Zero-Trust Vendor Access:** Treat all external connections—including those from long-term integrators or OEMs—as untrusted. Enforce granular, time-bound credentials and session monitoring for all remote maintenance.
- **Software Assurance and SBOM Visibility:** Require vendors to provide software bills of materials (SBOMs), validate digital signatures, and monitor for tampered or outdated components in updates.
- **Vendor Accountability:** Embed cybersecurity clauses into supplier contracts, mandating secure update practices, vulnerability disclosure, and immediate reporting of incidents that could affect OT environments.
- **Network Segmentation and Continuous Monitoring:** Ensure supplier-facing gateways are isolated from production networks, and maintain visibility over outbound traffic that could signal unauthorized data exchange or command activity.
- **Shared Threat Intelligence:** Participate in sector-specific information sharing (e.g., ISACs/ISAOs) to quickly identify supply chain compromises impacting industrial peers or upstream providers.

HISTORICAL CASE STUDIES

1) 2024 – Cyber Av3ngers Target Unitronics PLCs (Water and Other Sectors, U.S.)

Between late 2023 and 2024, an Iran-linked group known as Cyber Av3ngers exploited internet-exposed Unitronics PLCs in the water and wastewater sector and other small industrial environments. Attackers defaced HMI screens with political messages and occasionally modified PLC logic, highlighting the risks of default credentials and direct internet exposure. Several U.S. utilities were affected, prompting nationwide CISA and WaterISAC advisories.

Lessons learned: Eliminate direct internet access to control devices, change vendor-default passwords, enforce network segmentation and VPN gateways for maintenance access, and continuously monitor for unauthorized logic or configuration changes.

2) 2022 – Industroyer2 Attempt on Energy Infrastructure (Ukraine)

In April 2022, Russia's Sandworm Team deployed Industroyer2, a successor to the 2016 grid-attacking malware, against Ukrainian high-voltage substations. Swift defensive action by CERT-UA and ESET prevented a blackout. The malware's modular design and use of native OT protocols (IEC-104) demonstrated that state actors retain offensive capability to directly manipulate physical processes.

Lessons learned: Energy operators must harden substation networks with strict allow-lists, secure serial interfaces, and active protocol inspection. Joint incident-response exercises with OEMs and national CSIRTs remain essential for rapid containment and restoration.

3) 2021 – Colonial Pipeline Ransomware Incident (U.S.)

In May 2021, the DarkSide ransomware operation hit Colonial Pipeline's corporate IT systems, prompting a preemptive shutdown of OT operations to prevent lateral spread. The five-day outage disrupted 45 percent of East Coast fuel supply and triggered a federal emergency declaration. Though the OT network was not directly encrypted, interdependencies between business and operations functions made recovery complex.

Lessons learned: Build resilient interfaces between IT and OT, rehearse manual operations and restart plans, and ensure incident response can isolate IT systems without halting safe plant function.

4) 2021 – Oldsmar Water Utility Intrusion (Florida, U.S.)

In February 2021, an unknown actor accessed the Oldsmar water treatment plant's SCADA HMI via TeamViewer and briefly changed chemical dosage settings to unsafe levels. An operator noticed and reversed the change, preventing harm. While no damage occurred, the incident exposed weak remote-access controls common in small utilities.

Lessons learned: Limit remote-control software, require multifactor authentication, log HMI activity, and configure process alarms for out-of-profile setpoints.

5) 2020 – Natural Gas Compression Facility Ransomware (U.S.)

In early 2020, ransomware disrupted a U.S. natural gas compression facility's control and communication assets, causing a two-day shutdown and supply chain delays. The attack spread from IT into OT due to insufficient network segmentation and shared credentials.

Lessons learned: Implement robust IT/OT segmentation, regular backups for engineering workstations and controller configs, and comprehensive OT incident-response drills.

Sector context and takeaways (2020–2025)

Over the past five years, attacks on operational technology have evolved from accidental IT spillover to deliberate targeting of critical infrastructure by both criminal and state-sponsored actors. Energy and water sectors have borne the brunt, with themes of ransomware-driven disruption, remote-access abuse, and supply-chain weaknesses.

The Ukraine and Cyber Av3ngers cases underscore a trend toward hybrid warfare and geopolitical messaging through cyber-physical effects. For defenders, the imperatives are clear: build defensible OT architectures with minimal attack surface, maintain offline restoration paths, and foster public-private coordination to detect and respond before physical impact occurs.

DEFENSIVE POSTURE AND BEST PRACTICES

- Implement robust network segmentation following ISA/IEC-62443 standards, with dedicated security zones for OT networks and controlled access points between IT and OT environments. Deploy industrial firewalls and data diodes to prevent unauthorized lateral movement.
- Establish comprehensive monitoring using industrial protocol analyzers and behavioral analytics to detect anomalous communications within OT networks. Implement the NIST Cybersecurity Framework with OT-specific controls, focusing on asset inventory, vulnerability management, and incident response procedures.
- Secure remote access through multifactor authentication, privileged access management, and session monitoring. Regularly update and patch OT systems during planned maintenance windows, with thorough testing in isolated environments before production deployment.
- Develop OT-specific incident response procedures that account for safety considerations and operational continuity requirements. Train operational staff on cybersecurity awareness, emphasizing the unique risks associated with industrial control systems and the potential for cyber-physical attacks.

CONCLUSION

The April–September 2025 period demonstrated an increase in OT/ICS targeting, with sophisticated threat actors developing capabilities for industrial environments. The concentration of attacks on manufacturing and energy sectors, combined with the emergence of safety-system targeting, represents a critical threat to global infrastructure.

Organizations must prioritize OT security investments, implementing defense-in-depth strategies that account for the unique operational requirements of industrial systems. The evolution from opportunistic attacks to targeted campaigns against safety systems requires immediate attention to prevent potential catastrophic incidents that could result in loss of life and widespread economic disruption.

See more threat reports from Trellix Advanced Research Center.

This document and the information continued herein describes computer security research foreducational purposes only and the convenience of Trellix customers. Trellix conducts research in accordance with its Vulnerability Reasonable Disclosure Policy I Trellix. Any attempt to recreate part or all of the activities described is solely at the user's risk, and neither Trellix nor its affiliates will bear any responsibility or liability.

Trellix is a trademark or registered trademark of Musarubra US LLC or its affiliates in the US and other countries. Other names and brands may be claimed as the property of others.