Presented by

Trellix ADVANCED RESEARCH CENTER

OPERATIONAL TECHNOLOGY THREAT REPORT

October 2025–March 2026

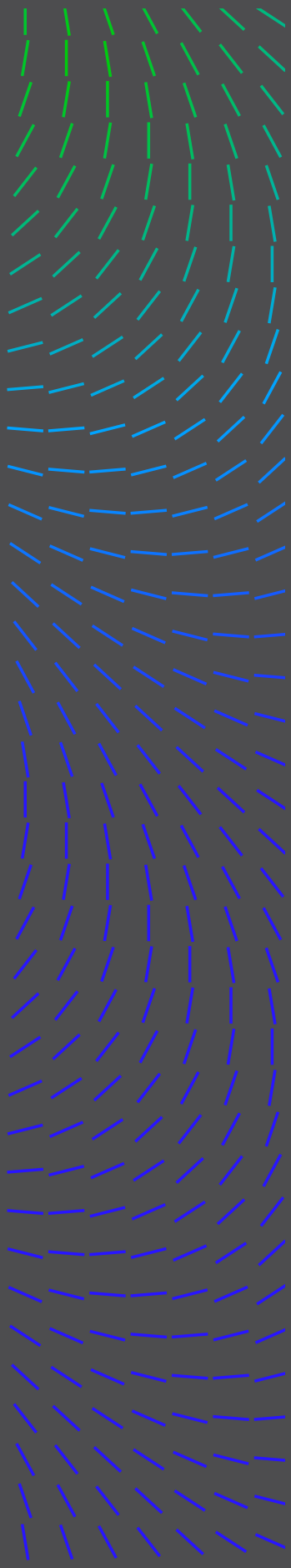
EXECUTIVE SUMMARY

From October 2025 to March 2026, Trellix telemetry recorded 1.3 million detections across 155 unique campaigns targeting operational technology (OT) and industrial control system (ICS) linked environments. According to the Trellix Ransomware Tracker, we observed 1,600+ OT-impacting attacks globally, representing 29.5% of all ransomware activity during the period.

Overall, ransomware victims increased 48.2% from October 2025 to February 2026—the peak month—before a post-peak correction in March, with the OT sector specifically experiencing a 46.2% surge over the same window. This measurable increase signals an accelerating threat landscape defined by the widespread exploitation of IT/OT boundary devices.

Nation-state actors, primarily Russia, China, and Iran, carried out targeted operations, with destructive wiper malware and deep network pre-positioning dominating the state-sponsored toolkit. Meanwhile, financially motivated syndicates weaponized the erosion of the traditional air gap. Ransomware groups continued to engage in "industrial extortion," exploiting internet-facing corporate IT systems to force downstream operational downtime across the manufacturing and energy sectors.

Ultimately, the convergence of geopolitical conflict, ransomware proliferation across IT/OT boundaries, and delayed industrial patching cycles presents a compounding risk to critical infrastructure operators worldwide.



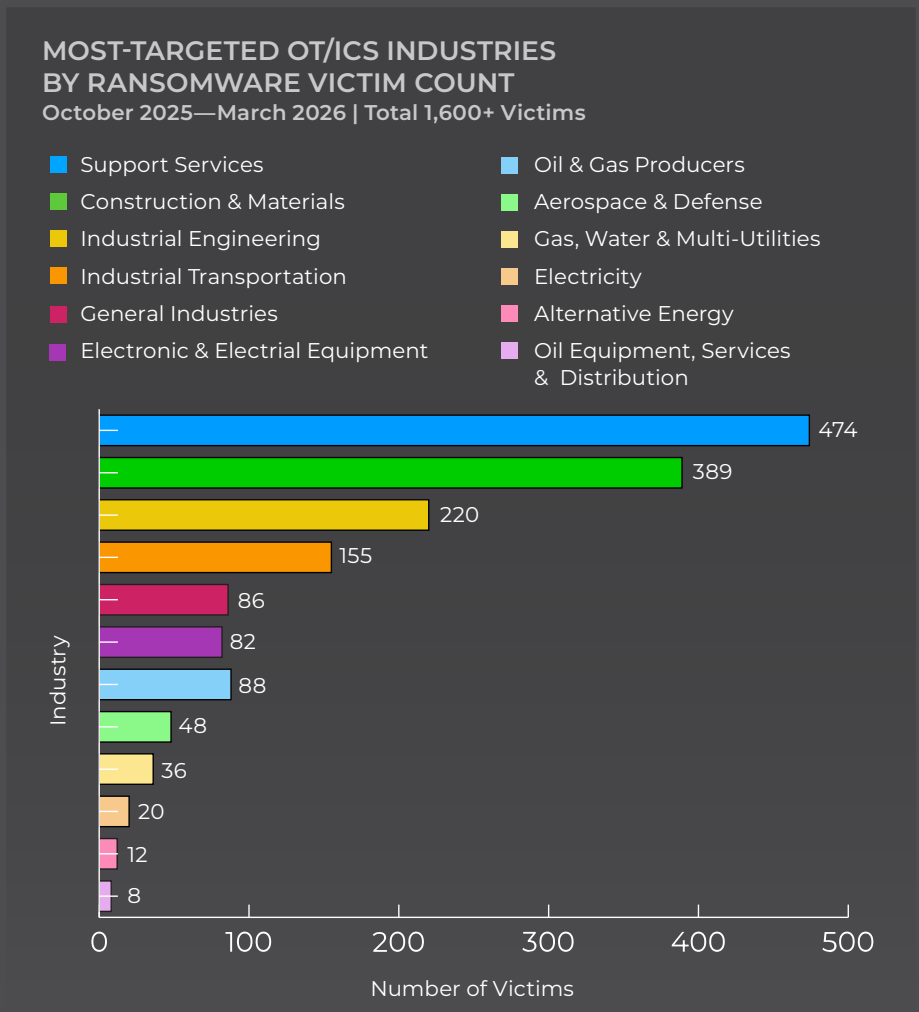
OT THREAT LANDSCAPE OVERVIEW

The OT threat landscape during this period was shaped by two converging forces: nation-state actors conducting deliberate, geopolitically motivated attacks on critical infrastructure, and financially motivated ransomware groups increasingly targeting industrial sectors. Russian threat actors, particularly Sandworm and Dragonfly, continued to deploy wiper malware against European energy infrastructure, directly linked to the ongoing Russia-Ukraine conflict and NATO's eastern expansion.

Supply chain risk emerged as a critical concern. Geopolitical tensions continued to shape sector-targeting patterns. Iran's MuddyWater explicitly targeted Israeli electric, gas, oil, and water sectors in parallel with the ongoing Middle East conflict. Chinese APT groups conducted systematic prepositioning operations across North American and Asian critical infrastructure, consistent with pre-conflict doctrine ahead of potential Taiwan Strait contingencies. Ransomware groups collectively claimed 1,600+ victims across industrials, oil and gas, and utilities during the reporting window, representing 29.5% of all ransomware activity during the period. This created measurable OT disruption risk as ransomware propagated across IT/OT convergence points.

Sector Targeting

The chart below shows the most-targeted OT/ICS sectors by ransomware victim count (October 2025–March 2026).



THREAT ACTOR ACTIVITY

Most active threat actors targeting OT

Dragonfly / Static Tundra (Russia)
Dragonfly (also Energetic Bear, Berserk Bear, Ghost Blizzard) is Russia's energy sector specialist, active since 2011. The group conducted a multisector destructive campaign against Poland's energy and manufacturing sectors in January 2026, deploying DynoWiper and LazyWiper alongside lateral-movement tooling. Dragonfly contributed 1,034 detections and is assessed as maintaining persistent access to multiple European energy operators.

Volt Typhoon (China)
Volt Typhoon is assessed by CISA, NSA, and FBI as prepositioning within US critical infrastructure for potential activation during a Taiwan Strait conflict. The group operates almost exclusively via "living-off-the-land" binary (LOLBin) techniques, making detection difficult. Multiple campaigns during this period targeted North American critical infrastructure with deep Active Directory reconnaissance.

MuddyWater (Iran)
An Iranian-linked state-sponsored group, MuddyWater, conducted two notable OT-sector campaigns during this period. Most notably, the group explicitly targeted Israeli electric, gas, oil, and water sectors, deploying updated RMM-abuse tooling and the MuddyViper backdoor. A second campaign deployed a novel Telegram-based C2 framework against energy and infrastructure targets. For more information on Iranian cyber capability, please check out this blog.

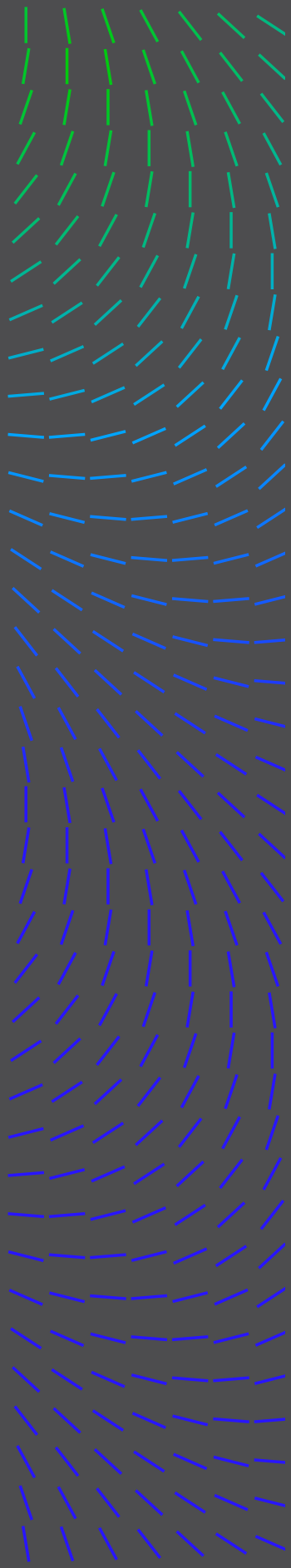
Qilin (Ransomware)
The most prolific ransomware group by OT victim count, Qilin claimed 328 OT-sector victims, with manufacturing, construction, and industrial machinery as primary targets. Qilin's high volume and broad industrial targeting make it a consistent OT disruption risk.

Akira (Ransomware)
Akira claimed 136 OT-sector victims between October 2025 and March 2026, with construction and materials as its primary target (34.6% of its OT total), followed by support services and industrial engineering.

Recent High-profile OT Campaigns

The modern industrial threat landscape is defined by the erosion of the IT/OT boundary. While some of the campaigns detailed below originated as compromises within corporate IT environments, they are included in this OT threat report because their primary impact was the degradation of operational technology, manufacturing availability, and downstream supply chains.

Qilin Ransomware—European Energy Infrastructure Disruption (Q1 2026)
A European energy and pipeline operator suffered a disruptive cyberattack claimed by the Qilin ransomware group. Qilin alleged the theft of a significant volume of internal data. The incident disrupted the operator's corporate IT systems and took public-facing infrastructure offline, though the organization confirmed its core SCADA and transport operations remained unaffected. Threat intelligence indicates the breach may have originated from an



infostealer infection on an IT administrator's dual-use personal device weeks earlier, granting attackers valid WSUS and VPN credentials to bypass perimeter defenses.

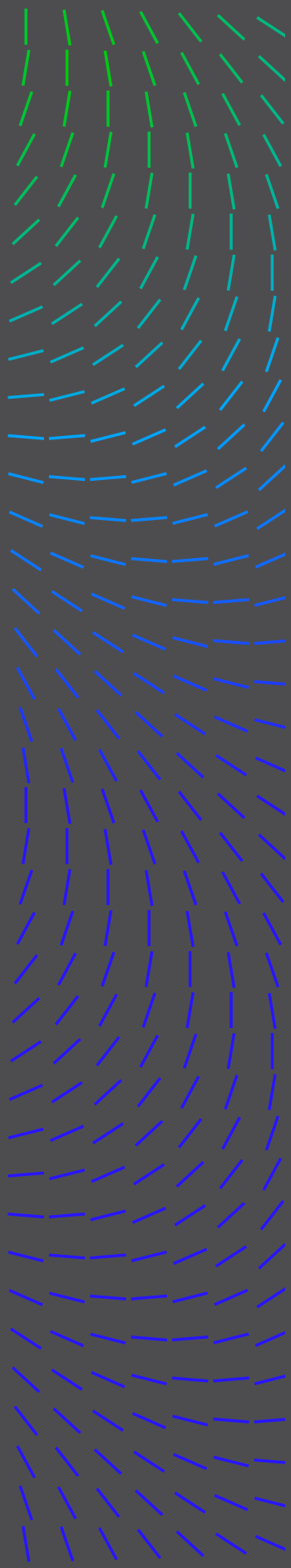
Handala Wiper Attack—Healthcare Manufacturing Disruption (Q1 2026)
A multinational medical technology manufacturer experienced a disruptive global cyberattack. The Iranian-linked hacktivist group Handala claimed responsibility, conducting a destructive wiping attack using a legitimate administrative tool to permanently delete data from tens of thousands of endpoints.

The attackers compromised a Windows domain admin account to create a new Global Administrator profile, misusing endpoint management systems to push the payload. The attack forced the manufacturer to deliberately disconnect major portions of its network, leading to widespread disruptions across its global manufacturing and shipping operations.

Iranian State-sponsored ICS Targeting Unitronics and Tridium (ongoing to March 2026)
Aligning with heightened geopolitical tensions in the Middle East, a March 2026 threat analysis by Censys revealed sustained, opportunistic targeting of internet-exposed ICS devices by Iranian actors. Throughout late 2025 and into March 2026, threat actors systematically probed Unitronics Vision PLCs, Orpak SiteOmat systems, Red Lion equipment, and Tridium Niagara frameworks. Multiple Iranian-linked hacktivist personas, including the IRGC-affiliated CyberAv3ngers, have historically exploited these systems via default credentials, reinforcing a growing trend of weaponizing internet-accessible OT boundary devices for retaliatory disruptions.

- During the final drafting of this report, the CISA, FBI, and NSA released a joint advisory AA26-097A detailing a newly discovered campaign by Iranian-affiliated APT actors. While this disclosure fell just outside our Q1 2026 reporting window, the intelligence confirms an ongoing escalation of the trends noted above. Threat actors targeted internet-facing programmable logic controllers (PLCs) manufactured by Rockwell Automation/Allen-Bradley—specifically CompactLogix and Micro850 devices—across the U.S. water, energy, and government sectors. By accessing the devices via exposed ports, attackers maliciously interacted with project configuration files and manipulated SCADA displays to cause operational disruption and financial loss. This incident strongly reinforces our strategic takeaway regarding the urgent need to remove PLCs from direct internet exposure.

Industrial Extortion—APAC Food and Beverage Manufacturer (Q4 2025)
The manufacturing sector experienced a sharp increase in ransomware in Q4 2025, heavily impacted by groups deliberately targeting production availability. A major Asia-Pacific (APAC) food and beverage manufacturer suffered a ransomware attack that caused direct operational disruption. The digital systems underpinning the company's business were taken offline, resulting in production halts at multiple factories. Threat intelligence reports classified this as a demonstrable case of "industrial extortion," where adversaries move beyond data encryption to weaponize manufacturing downtime.



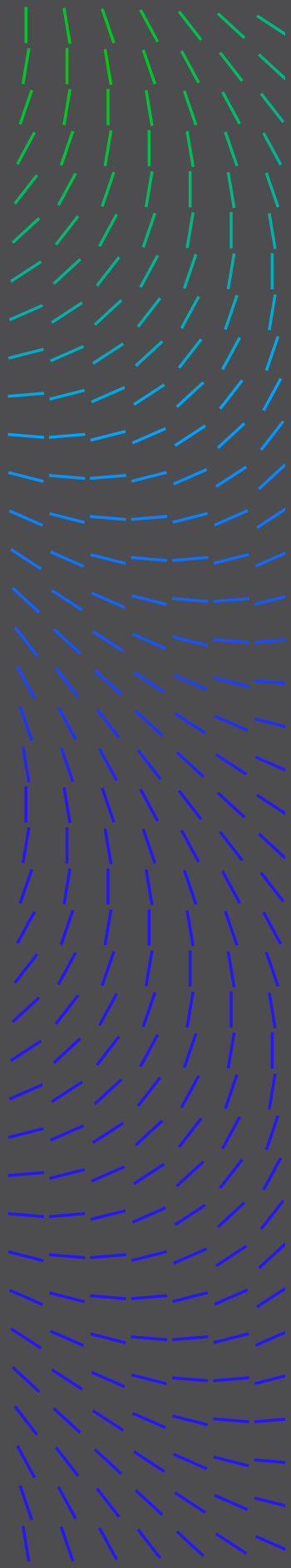
Consumer Goods Manufacturing and Shipping Cyberattack (Late Q1 2026)
Following a network intrusion detected in late March 2026, a multinational consumer goods manufacturer suffered an unauthorized breach of its IT infrastructure. To contain lateral spread, the company proactively shut down selected systems, resulting in immediate, multi-week impacts on its ability to accept orders, manage shipments, and run production operations.

UAT-8837—Critical Asian Infrastructure (March 2026)
The most recent campaign in our reporting window, attributed to UAT-8837, targeted civil aviation, energy, and telecoms across Asia. The group exploited public-facing IIS servers, deployed Godzilla webshells, and used the Sliver implant and Fast Reverse Proxy (FRP) for persistent access. Memory forensics tools (DumpIt, Volatility) were repurposed for credential extraction.

Dragonfly / Static Tundra—Multisector Poland Attack (January 2026)
This campaign, with attribution from Polish authorities, targeted Poland's energy and manufacturing sectors with the deployment of DynoWiper alongside a full-spectrum toolkit. Techniques included Advanced IP Scanner for OT network reconnaissance, Impacket and PsExec for lateral movement, Kerberos ticket forgery, and system firmware tampering. The group used TOR, Dropbox, Pastebin, and Slack for C2, a "living-off-the-cloud" evasion approach.

MuddyWater—Israeli Electric, Gas, Oil, and Water Sectors (December 2025)
Iran's MuddyWater group conducted a targeted campaign against Israeli OT utility sectors, deploying the MuddyViper and VAX-One backdoors alongside credential harvesting tools (Mimikatz, HackBrowserData). The group abused legitimate RMM tools, Atera, SimpleHelp, PDQ Connect, and Syncro, to maintain persistent access that blends with legitimate IT management traffic in OT environments.

Chaya_003—Siemens Process Terminator (Ongoing)
A novel malware campaign specifically designed to terminate Siemens industrial processes generated 1,558 detections during the period. The malware uses Discord as a C2 channel, an unconventional evasion technique for OT environments, and is classified as ICS malware, RAT, and Worm. Attribution remains unconfirmed.



TACTICS, TECHNIQUES, PROCEDURES (TTPS)

Top TTPs Observed (MITRE ATT&CK for ICS Mapping)

The dominant TTP profile across OT-targeting campaigns is destructive and wiper-oriented, consistent with state-sponsored sabotage objectives. The top detected techniques, with their MITRE ATT&CK mappings, are shown in the chart below.

TTP	MITRE ID	Detections	Context
File and Directory Discovery	T1083 / T1420 (ICS)	15,817	Pre-attack OT asset enumeration
File Deletion / Indicator Removal	T1070.004 / T1070	15,626	Anti-forensics post-compromise
Scheduled Task	T1053.005	13,405	Persistence and wiper deployment
Obfuscated Files or Information	T1027	11,036	Evasion across all actor types
System Information Discovery	T1082 / T1426 (ICS)	10,135	OT environment reconnaissance
PowerShell	T1059.001	9,705	Execution, Sandworm, MuddyWater
Disable or Modify Tools	T1562.001	9,291	Disabling OT security controls
Data Destruction	T1485 / T0831 (ICS)	8,481	Wiper deployment on OT systems
Disk Structure Wipe	T1561.002	8,242	MBR / partition destruction
Data Encrypted for Impact	T1486	8,076	Ransomware in OT environments
System Shutdown / Reboot	T1529 / T0816 (ICS)	7,117	Disruption of OT operations
Firmware Corruption	T1495 / T0839 (ICS)	6,497	Targeting PLCs, RTUs, modems

IT-to-OT Pivoting

IT-to-OT pivoting follows a consistent multistage pattern across campaigns. Adversaries first establish an IT foothold by exploiting public-facing applications (VPN appliances, IIS servers) or through spearphishing.

From the IT network, actors conduct reconnaissance using tools such as SharpHound (BloodHound), Advanced IP Scanner, and Shodan/Censys to identify OT-adjacent network segments and assets.

Credential harvesting via LSASS memory dumping (Mimikatz, Rubeus) and Kerberoasting then enables lateral movement into OT-adjacent systems via SMB, RDP, WMI, and PsExec. Protocol tunneling tools—Chisel, EarthWorm, Ligolo-ng, and FRP—are used to traverse network segmentation boundaries between IT and OT zones.

Once inside OT networks, actors deploy ICS-native protocol abuse (IEC-104, Modbus), firmware corruption, and wiper malware to achieve their objectives. The entire kill chain from initial access to OT impact has been observed in under one hour in the most aggressive campaigns.

VULNERABILITY AND EXPOSURE INSIGHTS

During the October 2025–March 2026 reporting period, the vulnerability landscape was defined by a convergence of persistent legacy industrial exposures and active exploitation of zero-days at the IT/OT boundary.

While adversaries continue to target specialized core industrial assets, such as Siemens process controllers (e.g., Chaya_003), Schneider Electric Safety Instrumented Systems, and Modbus-enabled PLCs, the primary initial breach points were internet-facing edge appliances like SonicWall, Ivanti, and Cisco VPNs.

Structural challenges in OT environments compound this risk. Human-machine interface (HMI) workstations running legacy Windows operating systems remain persistent exposures, frequently bridging IT and OT networks and falling victim to RDP and SMB lateral movement.

Because OT patching timelines are dictated by strict operational continuity requirements and vendor certification constraints, often stretching into months or years, adoption rates lag behind disclosure timelines. Industry data also reveals a growing percentage of high-severity flaws lacking official CISA advisories. Consequently, even known-vulnerable systems remain exposed for extended periods, giving adversaries a predictable window for exploitation.

1. The IT/OT Boundary: VPNs and Edge Appliances as the Primary Breach Point

Internet-facing edge devices intended to secure remote access have paradoxically become high-risk exposure points for OT environments. Threat actors prioritize these to bypass segmentation and achieve rapid IT-to-OT pivoting.

MongoDB "MongoBleed" Information Leak (CVE-2025-14847):
Disclosed in December 2025, this unauthenticated memory disclosure vulnerability affects the MongoDB Server. Researchers observed active, opportunistic exploitation campaigns shortly after disclosure. Attackers launched high-velocity network connections against internet-exposed servers to extract uninitialized heap memory and harvest plaintext database credentials, API keys, and session tokens.

- **OT Risk Connection:** MongoDB is increasingly used as backend storage for modern Industrial Internet of Things (IIoT) platforms, manufacturing execution systems (MES), and operational data historians. By successfully harvesting API keys and plaintext credentials

via MongoBleed, attackers acquire the exact privileges needed to pivot directly into the control layer, allowing them to quietly steal proprietary production metrics, alter manufacturing recipes, or disable operational alarms.

Fortinet FortiWeb WAF Command Injection (CVE-2025-64446): Disclosed and confirmed exploited in the wild in November 2025, this critical vulnerability allows an attacker to execute administrative commands on the system via crafted HTTP/HTTPS requests. Threat intelligence indicates widespread exploitation by initial access brokers (IABs) and ransomware affiliates since late 2025. Attackers are utilizing automated scanning pipelines to execute path traversal attacks targeting the internal cgi-bin endpoint. Their goal is to create unauthorized, persistent local administrator accounts (often using hardcoded usernames like "Testpoint" or "trader1") to establish a reliable backdoor for deeper network pivoting.

- **OT Risk Connection:** FortiWeb is frequently deployed to protect web-based HMIs and OT administrative portals. Compromising the web application firewall (WAF) provides attackers with a direct bypass of perimeter inspection. With a persistent, administrator-level backdoor established, threat actors can freely deliver malicious payloads, manipulate web-based HMI interfaces, or deploy ransomware directly to downstream industrial applications without triggering traditional perimeter alarms.

2. Industrial Control Software and Facility Exploitation

Vulnerabilities in software that links business systems to manufacturing processes, or manages facility-wide environments, serve as high-privilege pivot points into the core OT environment.

AVEVA Process-optimization Flaws (CVE-2025-61937 and CVE-2025-64691): Highlighted in CISA advisory ICSA-26-015-01 (January 2026), these critical vulnerabilities include an unauthenticated remote code execution (RCE) via the 'taoimr' service and a privilege escalation flaw via TCL Macro scripts.

- **OT Risk Connection:** Exploitation allows an attacker to execute arbitrary code and escalate privileges to the OS system level. This results in the complete compromise of the Model Application Server, the centralized software brain governing heavy manufacturing and process control.

Johnson Controls Metasys SQL / Command Injection (CVE-2025-26385): Disclosed in early 2026, this vulnerability affects multiple Metasys building automation components (ADS, ADX, NAE) deployed with SQL Express.

- **OT Risk Connection:** As a core facility management platform, Metasys controls HVAC, power, and environmental systems. Exploiting this network-accessible flaw allows unauthenticated remote SQL execution, enabling attackers to alter ventilation, disable safety thresholds, and suppress facility alarms across manufacturing plants, hospitals, and critical infrastructure.

Automated Logic WebCTRL Premium Server BACnet Flaws (CVE-2026-32666 and CVE-2026-24060): Disclosed via a CISA advisory in March 2026, these high-severity vulnerabilities affect WebCTRL, a premier building-automation platform. The flaws stem from the system inheriting the BACnet protocol's lack of network-layer authentication, allowing service information to be transmitted in cleartext.

- **OT Risk Connection:** As a core facility management platform, WebCTRL governs critical environmental controls, HVAC, and power routing for manufacturing plants and data centers. Because the system fails to validate BACnet traffic, an attacker with network access can easily spoof packets to impersonate communications, intercept traffic, or alter environmental thresholds. This allows threat actors to bypass traditional software security and cause physical facility disruptions without requiring initial administrative credentials.

3. Direct ICS/OT Protocol Exposures and Niche Systems

These critical flaws target physical controllers, smart gateways, and highly specialized infrastructure, representing the inherent risk in vendor product lines and unpatchable niche environments.

Radiometrics VizAir Airport Weather Monitoring (CVE-2025-61945, CVE-2025-54863, CVE-2025-61956): Reported via CISA ICS advisories in late 2025, these flaws involve missing authentication controls on the VizAir administrative panel.

- **OT Risk Connection:** VizAir systems provide real-time wind shear detection and weather decision support at airports. Unauthenticated access allows attackers to modify critical parameters such as wind shear alerts, inversion depth, and CAPE values. This unauthorized manipulation can disable vital alerts and mislead air traffic control, directly threatening aviation safety and causing potential runway incursions.

Iskra iHUB and iHUB Lite Missing Authentication (CVE-2025-13510): Disclosed in December 2025, this flaw reveals that the smart metering gateway exposes its web management interface without requiring authentication.

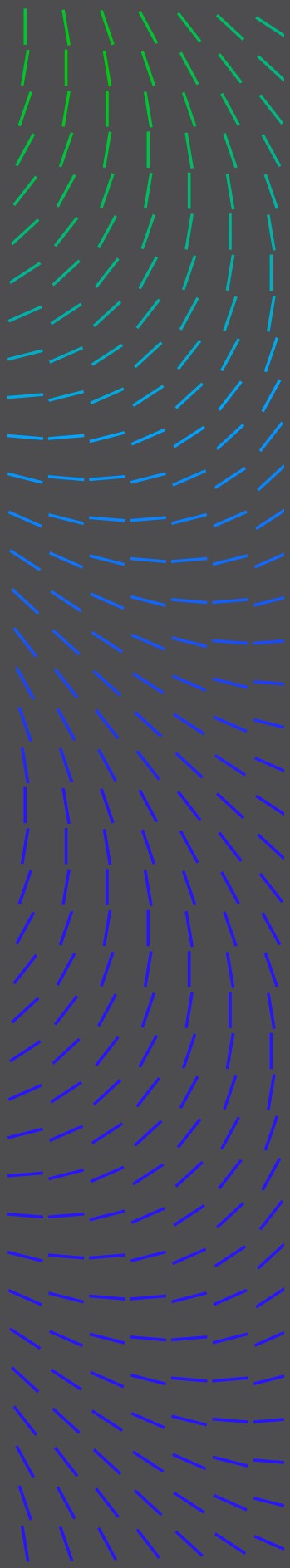
- **OT Risk Connection:** iHUB devices serve as essential data concentrators and communication gateways for smart grid and energy metering infrastructure. This flaw allows an unauthenticated attacker to directly access and modify critical device settings, reconfigure devices, and manipulate connected utility systems.

Strategic Takeaways

The IT/OT Edge Is the Primary Battleground: Internet-facing boundary systems, particularly VPNs and web application firewalls (WAFs), have become the weakest link in industrial security. The network perimeter is now the definitive zone of conflict for IT-to-OT pivoting.

Patch Latency Creates Predictable Exploitation Windows: The inherent delays in OT patch cycles transform months-old, high-severity vulnerabilities into reliable breach opportunities. Threat actors are routinely weaponizing this operational latency before vendor patches can be safely deployed.

A Tactical Shift Toward Data-Integrity Attacks: By compromising Level 3 orchestration systems (like MES or supervisory control), adversaries gain a "two-for-one" advantage: they harvest high-value credentials while establishing command over production. This signals a shift from obvious physical disruption to the corruption of production data, quality controls, and scheduling.



Unpatchable Risk Must Be Managed Architecturally: The persistent reality of legacy OT assets means foundational operational risk cannot be patched away. It must be chronically managed through architectural network controls, segmentation, and zero-trust principles.

Industrial Supply Chain Opacity Demands Deep Visibility: The active exploitation of specialized industrial software and niche infrastructure (like smart grid gateways and aviation weather controls) reveals a widening supply chain vulnerability. Maintaining resilience requires granular visibility into software components and continuous monitoring for anomalous network behaviors.

HISTORICAL LESSONS APPLIED TO MODERN DEFENSE

The most effective way to anticipate modern operational technology threats is to examine the tactical blueprints established by early nation-state campaigns. While geopolitical adversaries, such as those aligned with Iran, China, and Russia, have distinct strategic motivations, the mechanics of how they compromise critical infrastructure have converged. By analyzing these foundational incidents, we can identify the common denominators driving today's threat landscape and directly apply those lessons to our current defensive strategies.

Instead of treating these historical breaches as isolated anomalies, we must recognize them as the origins of today's most prevalent attack vectors. Threat actors have realized that custom, highly complex ICS malware is often unnecessary. Today, they are weaponizing the IT/OT boundary, "living off the land," and using IT disruption to force physical downtime. The case studies below highlight how historical nation-state tactics have evolved into the ubiquitous threats facing industrial operators today.

Iran and the Playbook for IT-induced OT Downtime

In 2012 and 2016, Iranian state-sponsored actors deployed the highly destructive Shamoon wiper malware against Saudi Aramco and other Middle Eastern petrochemical companies. While the malware primarily destroyed corporate IT networks, wiping tens of thousands of workstations, the extensive loss of IT infrastructure forced prolonged operational shutdowns.

Modern Application: Today, this "industrial extortion" playbook is the exact model used by financially motivated ransomware syndicates. Attackers no longer need to engineer complex ICS payloads; they simply encrypt bridging IT systems (like billing, logistics, or safety monitoring) to force a plant to halt production. Defense strategies must account for this reality by engineering OT environments capable of "islanding" themselves, ensuring that critical physical processes can safely continue, or fail safely, even if the corporate IT network is entirely compromised or destroyed.

Iran and the Exploitation of Unsecured Edge Infrastructure

During the 2020 attacks on Israeli water facilities, and later in the 2023 CyberAv3ngers campaigns targeting Unitronics systems across the U.S. water sector, Iranian threat actors demonstrated an efficient attack path: exploiting internet-facing industrial systems with weak or default credentials. By targeting exposed edge devices, they bypassed traditional IT environments entirely to manipulate physical controllers directly.

Modern Application: The common denominator across today's threat landscape is that the network edge is the primary target. Just as Iranian actors exploited exposed PLCs for direct disruption, Chinese state-sponsored actors (like Volt Typhoon) now systematically exploit edge routers, firewalls, and VPNs for stealthy prepositioning. Organizations must stop treating legacy internet-facing devices as trusted boundaries and aggressively transition toward zero trust network access (ZTNA) architectures that remove these vulnerable assets from the public internet.

Russia, China, and the Shift to "Living off the Land"

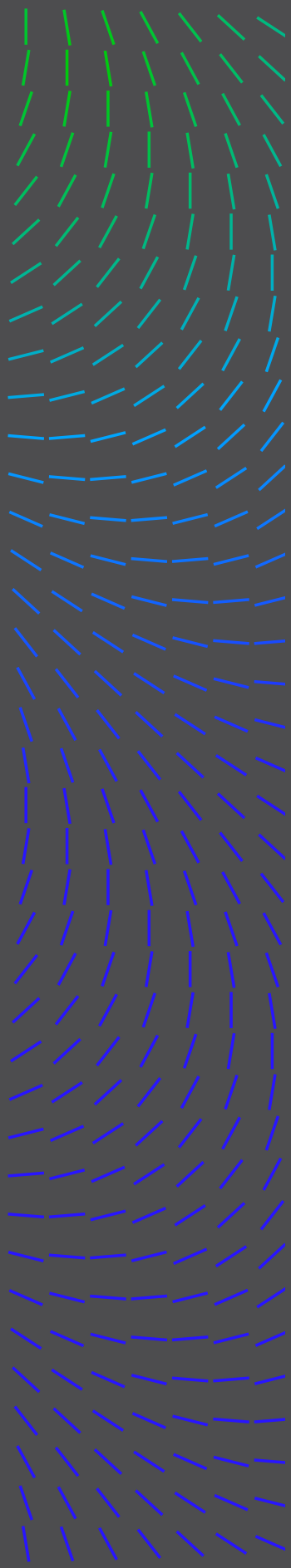
When Russian actors (Sandworm) attacked the Ukrainian power grid in 2015 and 2016, the defining characteristic wasn't just their use of custom malware like Industroyer; it was their heavy reliance on stolen credentials, VPN access, and native IT tools to pivot and map the OT environment before dropping their final payloads.

Modern Application: This historical shift away from custom exploits has become the standard operating procedure for modern adversaries, particularly Chinese groups seeking long-term persistence without detection. By "living off the land" (LotL), abusing native Windows administration tools, legitimate remote monitoring (RMM) software, and unencrypted industrial protocols like Modbus or BACnet, threat actors seamlessly blend into normal network traffic. To counter this, defenders must move beyond purely signature-based malware detection and adopt deep, protocol-level behavioral analytics to detect malicious use of legitimate tools.

DEFENSIVE POSTURE AND BEST PRACTICES

Enforce Strict IT/OT Boundary Defenses and Segmentation: Following ISA/IEC-62443 standards, establish dedicated security zones and eliminate direct IT-to-OT connectivity. Crucially, prioritize the hardening and rapid patching of internet-facing edge appliances (VPNs, WAFs) and consider migrating to Zero Trust Network Access (ZTNA), as vulnerable perimeter devices remain the primary breach point for ransomware IT-to-OT pivoting.

Deploy OT-aware Visibility and Restrict Dual-use Tools: Implement continuous monitoring using industrial protocol analyzers to detect anomalous read/write commands (e.g., Modbus, IEC-104). To counter the "living off the land" techniques and RMM abuse (Atera, AnyDesk) prevalent in recent nation-state campaigns, strictly audit administrative tools, restrict PowerShell execution, and block unauthorized protocol tunneling across network segments.



Harden Identity Infrastructure and Remote Access: Mandate phishing-resistant multifactor authentication (MFA) and privileged access management (PAM) for all internal and third-party remote access. Because adversaries rely heavily on credential harvesting (e.g., LSASS dumping) for lateral movement, organizations must aggressively monitor and isolate Active Directory environments that bridge IT and production domains.

Implement Risk-based Vulnerability and Supply Chain Management: Acknowledge that OT patching timelines are inherently delayed. Prioritize compensating network controls (such as data diodes or targeted firewall rules) around critical, unpatchable Level 3 industrial software (e.g., SCADA, MES). Additionally, strictly audit third-party vendor access to mitigate the risks associated with compromised ICS supply chains.

Develop Destructive-event Incident Response Plans: Evolve OT-specific incident response playbooks to explicitly account for simultaneous IT data destruction and OT physical disruption, as demonstrated by the proliferation of wiper malware. Maintain offline, frequently tested backups of critical engineering assets, including PLC/RTU logic, HMI configurations, and historian data, to ensure rapid recovery from industrial extortion or sabotage.

CONCLUSION

The October 2025—March 2026 reporting period highlights a measurable shift in how adversaries target OT and ICS environments. Nation-state actors are expanding their prepositioning operations, while ransomware syndicates exploit the eroding IT/OT air gap. The rise of "industrial extortion" demonstrates that attackers no longer require purpose-built ICS malware to cause physical downtime; breaching perimeter IT appliances is now a proven, efficient method for halting downstream production.

Addressing the convergence of state-sponsored activity, ransomware proliferation, and inherent OT patch latency requires defensive strategies tailored to industrial networks. Operators must transition to an intelligence-led defense by treating IT/OT boundary devices as primary attack surfaces, isolating unpatchable legacy assets, and enforcing strict network segmentation to prevent lateral movement.

The adversaries documented in this report are highly adaptive and strategically motivated. Notably, the ongoing geopolitical conflict involving Iran remains a persistent concern, driving state-aligned actors and hacktivists to conduct retaliatory, opportunistic disruptions against critical infrastructure globally. Organizations must counter this reality with a sustained, board-level commitment to OT resilience, grounding their security posture in practical, architectural standards such as ISA/IEC-62443 and the NIST Cybersecurity Framework.