



OT-ISAC

OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

Maritime Actionable Intelligence Report: Shipyard Vulnerabilities, OT Threats & Global/APAC Updates (TLP Clear)

Report Date: November 3, 2025

Scope: Focus on shipyard and maritime-sector risks, emphasizing APAC (e.g., South China Sea tensions, regional APT activity), with global extensions. Intelligence draws from recent advisories, threat actor TTPs, OT safety impacts, and IoCs. Prioritises actionable steps for shipbuilders, operators and ports to mitigate disruptions, IP theft and safety hazards.

1. Key Vulnerability Advisories for Shipyard and Maritime Devices

Recent advisories highlight critical flaws in manufacturing and OT systems used in shipyards and vessels. Shipbuilders should prioritise patching and network hygiene, since exploitation could halt production lines or compromise vessel designs.

Vulnerability	CVSS Score / Comments	Affected Devices/Systems	Potential Impact on Shipyards/Maritime	Actionable Mitigation
Kaleris Navis N4 Terminal Operating System – CVE-2025-2566 (ULC unsafe Java deserialization → RCE)	CVSS v3.1: 9.8 (Critical); CVSS v4.0: 9.3 (Critical); unauthenticated remote code execution against the ULC service.	Navis N4 TOS Ultra Light Client (ULC) server components (widely deployed in container terminals).	TOS compromise → manipulation of yard jobs/equipment dispatch; outage with cascade to gate, yard, and quay operations.	Patch per CISA/Kaleris; place ULC behind an application gateway/reverse proxy; restrict admin consoles to jump hosts + MFA; add WAF rules for serialized payloads; integrity checks on TOS data.
Hitachi Energy TropOS industrial wireless – multiple vulns (incl. command)	CISA advisory (2025-10-30); remotely exploitable flaws; treat as High–Critical for port/yard meshes.	TropOS mesh radios (edge/core) used across ports, terminals, and industrial campuses.	Radio compromise → loss of mesh integrity, telemetry tampering, pivot into OT VLANs and remote-access paths.	Apply vendor fixes; disable unauth paths; restrict management to OT jump hosts + MFA; rotate keys/certs; monitor for config/firmware changes; segment TropOS

injection / priv-esc)				management from production VLANs.
Schneider EcoStruxure OPC UA Server Expert / Modicon Communication Server – CVE-2024- 10085 (CWE- 770 DoS)	High (Availability); unauthenticated request floods exhaust resources; fix in Server Expert SV2.01 SP3+.	EcoStruxure OPC UA Server Expert (pre-SV2.01 SP3) and Modicon Communication Server (listed affected versions). Common on engineering subnets bridging PLCs/HMIs.	HMI/recipe deployment delays; timeouts on engineering workflows; operations disruption even without code execution.	Patch to SV2.01 SP3+; place UA servers behind OT firewalls/DMZ; enforce client allow-lists; rate-limit sessions; forward UA audit logs and alert on spikes in CreateSession/ActivateSession.
Siemens SIMATIC RTLS Locating Manager – CVE-2025- 40746 (backup- script input validation → RCE)	CVSS v3.1: 9.1 (Critical); authenticated high- priv user in app can execute code as NT AUTHORITY\SYSTEM ; update to V3.2+.	SIMATIC RTLS Locating Manager < V3.2 (used for asset tracking in yards/warehouses).	RCE on RTLS server → falsified asset locations, disruption of yard workflows; potential pivot to adjacent systems.	Upgrade to V3.2+ per Siemens ProductCERT/CISA; restrict RTLS admin roles; network-isolate RTLS from production control VLANs; monitor for suspicious backup-script activity.
Dassault Systèmes DELMIA Apriso (MOM/MES) – multiple vulns (KEV- listed)	Exploited in the wild (CISA KEV). Specific CVEs include recent code- injection/deserializa- tion issues disclosed in 2025. Prioritize if Apriso is in your yard stack.	Shipyards only: DELMIA Apriso- based MOM/MES used to monitor/execute shipyard production; not typically deployed onboard vessels.	Compromise of MOM/MES → manipulation of work orders, quality records, materials and scheduling; potential knock-on effects into TOS/warehouse/R TLS integrations.	Apply vendor patches immediately; restrict MOM admin to jump hosts + MFA; isolate MOM from OT control VLANs; monitor for unusual job/workflow changes; review integrations (PLM/ERP/TOS) for least privilege.
Citrix NetScaler ADC / Gateway – CVE-2025- 5777 ("CitrixBleed 2"), CVE- 2025- 7775/7776, CVE-2025- 8424	Critical. CVE-2025- 5777 (memory over- read/session theft) and CVE-2025-7775 (memory overflow → RCE/DoS) are KEV-listed / exploited in the wild. Older 12.1/13.0 builds are EoL.	Internet-facing remote-access gateways used for ship-to- shore/vendor access, OEM remote support, and crew access (some terminals/vendors standardize on NetScaler).	Credential/session theft or RCE on the gateway → direct hop into TOS/port IT; potential staging point toward OT jump hosts/vendor tunnels.	Patch immediately per Citrix bulletin; remove/upgrade EoL 12.1/13.0; rotate sessions/creds; restrict Gateway/AAA exposure; enforce MFA, Geo/IP allow-lists; monitor for anomalous AAA auths and config diffs.

Emerson Fisher ValveLink (SNAP-ON, SOLO, PRM, DTM) – ICSA-25-189-01 (multiple CVEs)	CVSS up to 8.5 (High); affects all ValveLink variants < v14.0; vendor and CISA issued fixes.	Valve diagnostics/config tools used with FIELDVUE positioners in yards, offshore, and process units connected to maritime ops.	Abusing ValveLink on ENG workstations can alter diagnostics/configs, enable unauthorized changes, or enable lateral movement via engineering tooling.	Upgrade to ValveLink ≥ 14.0; run as non-admin, sign/allow-list binaries; isolate ENG workstations from corporate; monitor ValveLink process launches and unexpected device config writes.
Microsoft WSUS – CVE-2025-59287 (unauth RCE) + OOB patches (Oct 23–24, 2025)	CVSS 9.8 (Critical); actively exploited; Microsoft shipped out-of-band fixes; CISA issued alert.	On-prem WSUS servers commonly used by ports/shipyards to patch Windows HMIs/ENG laptops and TOS servers.	Unauth RCE as SYSTEM on WSUS → full domain pivot; poisoning update channels to OT-adjacent hosts.	Apply Microsoft OOB updates (KB5070881/82/84/... per OS); remove Internet exposure; restrict 8530/8531/TLS to mgmt subnets; enforce TLS mutual auth/least-privilege; monitor for suspicious WSUS API calls & web logs.

APAC/Global Note: Shipyards in APAC (e.g., Singapore, South Korea) face heightened risk due to integrated supply chains and vendor networks. Globally, a large portion of vessel fleets remain on legacy Windows 10 post-end-of-support, amplifying OT exposure.

2. Threat Actor Activity Targeting Shipyards and Maritime

State-aligned APTs dominate the threat landscape, with APAC as a hotspot (e.g., South China Sea tensions). The focus is on espionage (IP theft of vessel/yard designs) and disruption (supply-chain, logistics). Shipbuilders must treat cyber as part of manufacturing risk.

Threat Actor / Group	Attribution / Origin	Targets in Maritime/Shipyards	Known TTPs	APAC/Global Activity (2025)	Actionable Defence
SideWinder (T-APT-04 / Rattlesnake)	Suspected India-origin	Ports, maritime authorities, logistics in South/Southeast Asia and Med.	Legacy Office exploit chains (e.g., CVE-2017-11882), spear-phishing; newer PDF/ClickOnce loader chains;	Continued espionage against maritime-adjacent orgs; infrastructure updates through 2024–2025.	Block MSI/ClickOnce; filter RTF/OOXML exploit lures; hunt unsigned DLL loads by signed binaries on ENG subnets.

			DLL sideloading.		
Mustang Panda (Earth Preta)	China-aligned	Gov/NGO and transport/logistics, incl. some maritime firms (EU/APAC).	USB-propagating loaders/worms ; PlugX/DOPLUG S DLL sideloading; phishing in legitimate packages.	2024–2025 activity spans EU & APAC; reports include cargo shipping/logistics victims in Europe.	Enforce USB lockdown/whitelists; detect DLL sideloading in EDR; app-control on ENG/TOS hosts; block outbound C2 families.
APT28 (Fancy Bear)	Russia (GRU)	NATO-aligned logistics; port/terminal vendor chains and transport tech ecosystems (adjacent).	Password spraying; Exchange permission abuse; WinRAR CVE-2023-38831; SOHO/router proxying.	Active 2022–2025 campaign vs logistics & tech.	Strict MFA on O365/IdP; monitor mailbox permission changes; block WinRAR exploit artifacts; egress controls on SOHO/edge routers.
Iran-aligned hacktivist activity (claim-driven)	Various	Iranian tanker comms and maritime logistics (claims)	Service-provider supply-chain compromise claims; comms disruption; data leakage (claims not yet officially adjudicated).	2025: multiple posts on tanker comms outages; treat as credible but partially corroborated.	Validate third-party satcom/teleport dependencies; monitor for comms anomalies; incident-ready fallback procedures.
Qilin ransomware	Russian-language ecosystem (public attribution varies)	Critical sectors incl. logistics/TOS suppliers; indirect impact to ports/shipyards.	Double-extortion (exfil + encrypt); supplier pivot to terminals.	~700+ claimed victims in 2025; high activity noted by Talos.	Offline, immutable backups; restore drills for TOS/ENG workstations; vendor hardening & incident-response clauses.

APAC/Global Note: While exact numbers vary, industry commentary reports a sharp rise of OT-adjacent targeting in the APAC maritime sector over 2024-25. The convergence of vessel IT/OT, legacy systems and increasing geopolitical tension elevates supplier and shipyard risk.

3. Operational Technology (OT) Alerts

OT systems in ships and shipyards (cranes, navigation, ballast, propulsion) remain high-value targets. Segmentation and specialist OT skills are still uneven across the sector.

- **Alert 1 — PRC-manufactured STS cranes:** USCG MARSEC 105-4 (Feb 2024) and 105-5 (Nov 2024) mandate cyber risk-management actions for PRC-made STS cranes; U.S. sources estimate ~80% of U.S. STS cranes are ZPMC.
Action: Segment crane networks; restrict & monitor vendor remote access; physically secure PLC/SCADA cabinets.
- **Alert 2 — GNSS spoofing/jamming:** UKMTO logged numerous interference reports (Oct 2025) in the Red Sea/Persian Gulf; global datasets show a continuing rise (2021–2025). Risk extends to congested APAC sea lanes.
Action: Implement bridge SOPs per Maritime Global Security (2025); monitor GNSS anomalies; cross-check INS/radar/visual fixes.
- **Alert 3 — Windows 10 EoS exposure in OT-adjacent hosts:** Windows 10 ended support on 14 Oct 2025; reliance on Win10 HMIs/engineering laptops elevates ransomware and pivot risk.
Action: Migrate to Windows 11 LTSC or hardened Linux; where upgrades aren't feasible, enroll in ESU and apply compensating controls (allow-listing, least-privilege, network isolation).
- **Guidance — Maintain a definitive OT architecture view:** CISA + UK NCSC (29 Sept 2025) advise keeping an authoritative OT asset/architecture view to enable anomaly detection and incident response.
Action: Maintain an accurate IT/OT inventory and data-flows; monitor for anomalous outbound & remote-control traffic.

4. Safety Impacts & Regulatory Updates

Cyber incidents in the maritime domain can escalate beyond downtime to collisions, groundings, environmental spills, and crew safety impacts – especially when navigation assurance or cargo-handling systems are affected. GNSS spoofing/jamming has been repeatedly reported in key waterways (e.g., Red Sea/Strait of Hormuz), with European authorities also documenting Baltic-Sea impacts.

- **Safety Risks:** OT breach → loss of propulsion, steering or cargo-handling integrity; GPS spoofing → vessel drift/grounding in crowded straits.
- **Regulations & Standards:**
 - **IMO/MSC – Resolution MSC.428(98):** Cyber risk management must be incorporated into the vessel SMS. (Adopted 16 Jun 2017.)
 - **IMO – MSC-FAL.1/Circ.3/Rev.3 (4 Apr 2025):** Updated Guidelines on maritime cyber risk management (high-level recommendations + functional elements).

- **IACS – UR E26 “Cyber Resilience of Ships” / UR E27 “Cyber Resilience of On-Board Systems & Equipment”**: Entry into force for new construction: 1 Jul 2024 (Rev.1). Increasingly used as baseline in newbuild contracts.
- **United States – USCG Final Rule “Cybersecurity in the MTS”**: Published 17 Jan 2025; effective 16 Jul 2025. Establishes minimum cybersecurity requirements (e.g., governance roles, incident reporting, assessments/training timelines) for U.S.-flagged vessels and MTSA facilities.
- **EU – NIS2 Directive (transport sector)**: If operating in or serving the EEA, entities in the transport sector fall under NIS2 risk-management and reporting obligations; align corporate controls accordingly.
- **Actionable Measures:**
 - **Assign accountability**: Appoint a Cybersecurity Officer / responsible officer per jurisdiction (e.g., USCG Final Rule for U.S. context).
 - **Embed into safety**: Align the vessel SMS with MSC.428(98) and the Rev.3 Guidelines; explicitly include navigation assurance (GNSS contingency) and cargo-handling cyber controls.
 - **Design to newbuild baselines**: For new tonnage or major refits, map requirements to IACS UR E26/E27 at specification stage.
 - **If EEA-exposed**: Plan NIS2 conformance checks (governance, supplier risk, incident reporting) for transport-sector entities.

5. Indicators of Compromise (IoCs) & Detection

While maritime-specific publicly disclosed IoCs remain limited, the following patterns are emerging and should be ingested into SIEM/EDR/OT-monitoring systems.

IoC / Signal Type	Examples / Details	Associated Threats	Detection Tools / Actions
IP / Domains (infrastructure)	Dynamic-DNS or low-reputation C2 domains; SOHO/router proxied IPs seen in recent GRU logistics campaigns.	APT28/GRU (logistics-focused 2022–2025), others.	Ingest IoCs from the joint CSA; block at egress; create SIEM rules for new destinations + dynamic-DNS from TOS/ENG subnets; alert on traffic transiting edge/SOHO routers.
File hashes / loaders	PlugX / DOPLUGS DLL sideloading; removable-media loaders/worms (e.g., PUBLOAD/HIUPAN variant chains).	Mustang Panda / Earth Preta.	Maintain YARA/Sigma for PlugX/DOPLUGS artifacts; EDR policy: quarantine unsigned MSI from removable media; block auto-run; USB whitelisting on ENG/TOS hosts.

Phish / doc-exploit artifacts	Legacy Office exploit chains (e.g., CVE-2017-11882), newer ClickOnce/PDF loaders; DLL sideloading trails.	SideWinder targeting ports/maritime facilities.	Mail-gateway rules for 11882 lure artifacts; block MSI/ClickOnce from email context; hunt unsigned DLL loads by signed binaries on engineering subnets.
Network patterns (IT→OT blast radius)	Unexpected WSUS (TCP 8530/8531) from OT zones; anomalous Exchange/WinRAR CVE-2023-38831 follow-on traffic; spikes to OPC UA (TCP 4840) from new clients.	Ransomware staging; APT28 tradecraft; OPC UA probing/DoS.	Monitor for WSUS to Internet or lateral from OT; flag WinRAR exploit artifacts + post-exploit egress; alert on bursts of CreateSession/ActivateSession to UA servers.
Endpoint / log changes	Credential-dump attempts on ENG workstations; new local-admin group members; suspicious signed-binary loads (e.g., rundll32, msixec) performing network egress.	Espionage footholds (APT28, SideWinder), ransomware precursors.	EDR detections for LSASS access; weekly privileged-account diffs; rules for signed-binary-proxy egress from ENG/TOS subnets.
Operational signals (navigation)	GNSS interference: sudden multi-NM jumps, GNSS source swaps, AIS/COG/SOG inconsistencies (Red Sea / Hormuz clusters in Oct 2025).	Actor varies; safety-critical.	Bridge/port monitoring for GNSS anomalies; correlate with UKMTO advisories; drill INS/radar/visual cross-checks.

6. Other Updates & Recommendations

- **APAC focus:** ReCAAP reports elevated incident levels in 2025 versus 2024; however, Q3 2025 saw a sharp decline after arrests by Indonesian authorities. Continue physical security and watchkeeping measures alongside cyber controls.
- **Global trend (USCG CTIME 2024):** USCG notes more cyber incidents and Coast Guard CPT missions involving cloud systems/services, plus supply-chain risks touching port equipment ecosystems. Expect increased attention on vendor/cloud assurance.
- **Capacity-building in Africa (Mauritania example):** IMO led a Sept 2025 needs-assessment mission at Port of Nouakchott on port digitalization/security; UN programs (UNOCT/UNODC) continue maritime/energy security training in Mauritania.
- **Immediate Actions for Shipbuilders/Ports:**

- Run OT vulnerability scans (e.g., aligned to National Institute of Standards and Technology SP 800-82 r3).
- Conduct quarterly crew/yard staff phishing and USB-usage awareness sessions.
- Join maritime cyber-info-sharing groups (e.g. OT-ISAC, MTS-ISAC).
- Simulate ransomware and OT-failover drills; aim for full recovery in < 24 h for critical systems.