OT-ISAC CLEAR *– Recipients may share* ***TLP:CLEAR*** *information without restriction.* ***TLP:CLEAR*** *information may be distributed freely, subject only to copyright controls. It is suitable for public release, including to media, the wider community, and external stakeholders, because it poses no foreseeable risk of misuse in its current form.*

OT-ISAC Threat Intelligence Report:

Land Transport Sector

This information is provided as-is for informational purposes only and comes with no expressed or implied warranties. You (and any individual or entity you represent) bear full responsibility for all actions and omissions made based on this information. OT-ISAC disclaims any responsibility or liability for any such actions or omissions.

In the spirit of community-driven effort, we'd like to encourage our Members and Partners to share information to enable our community better to defend itself and improve situational awareness. ***Most importantly - If your organization requires direct assistance from OT-ISAC, feel free to reach out to us directly - our team will work with you to ensure all necessary support is available through the member submission and RFI process.***

Executive Summary

Over the last year, land-transport OT risk has been defined by (1) criminal extortion incidents that disrupted passenger-facing operations in the Americas; (2) geopolitically driven nuisance/pressure activity and a major, non-cyber grid failure that immobilized rail/metro in Europe; and (3) steady ransomware pressure and technical OT faults in APAC. A newly disclosed End-of-Train/Head-of-Train (EoT/HoT) radio-link weakness (CVE-2025-1727) materially increases cyber-physical risk for freight operations globally if left unmitigated.

Bottom line*: Prioritize IT→OT containment, fix legacy unauthenticated train-control links, harden dispatch/signaling/SCADA against ransomware, and rehearse manual operations.*

Key Judgments

Judgment	Confidence	Supporting Evidence / Context
Ransomware remains the dominant cyber threat to North-American rail and metro operators; several IT breaches caused operational outages (e.g., *MTA Maryland 2025*).	High	Confirmed double-extortion cases with partial OT impact; continuity via manual dispatch maintained.
Rail-specific cyber-physical exposure increased following disclosure of weak EoT/HoT radio-link authentication (CVE-2025-1727); exploitation could trigger emergency braking on freight lines.	High	CISA ICS advisory (2025-280-01) and vendor tests proving unauthenticated stop-command feasibility.
Europe's most disruptive rail events were non-cyber, notably the Iberian Peninsula blackout halting metros across Spain and Portugal, but hacktivist DDoS remains persistent background noise.	High	ENTSO-E and EU reports attribute outage to grid instability; concurrent DDoS on rail portals detected.
Asia-Pacific maintains a high baseline of attacks and technical faults, with under-reporting of OT-specific compromises masking full impact.	Moderate	Regional CERT telemetry shows repeated ransomware attempts; public transparency limited.
IT–OT convergence continues to amplify risk; attackers breach IT (email/VPN) and pivot laterally to signaling or SCADA assets.	Moderate	Observed in 2024–25 ransomware playbooks targeting shared credentials and flat VLANs.
Data theft and extortion trends intensify, with adversaries exfiltrating employee PII and engineering data before encryption.	High	Rhysida, LockBit campaigns against transit agencies confirmed data-leak phases pre-ransom.
Legacy and proprietary rail OT systems remain difficult to secure, extending vulnerability windows.	Moderate	Long refresh cycles; outdated OS in interlockings; insecure serial/relay links in metros.

Incidents & Trends

Cyber Incidents

Date	Region	Incident & Actor	Impact on OT / Operations
Aug–Oct 2025	US	Maryland Transit Administration – Rhysida claims data-theft; state confirms cyber incident; paratransit booking degraded; real-time bus tracking affected during recovery.	Service degradation (MobilityLink bookings) and data exposure; core rail/bus ran with workarounds.
Dec 19–24, 2024	US	Pittsburgh Regional Transit – ransomware; initially "glitch," later confirmed; light-rail service halted for a day.	Short-term rail halt; manual fallbacks; recovery over days.
Mar–Jul 2025 (trend)	Europe	Hacktivist DDoS (NoName057(16)) targeting gov/transport portals; EU-led operation Eastwood disrupted its infra in July.	Online info/ticketing interruptions; no confirmed safety-system impact.

Note: Additional US/Canada municipal transit cyber events occurred but were minimally disclosed; patterns align with double-extortion and IT→OT precautionary slowdowns.

Non-Cyber OT/Technical Events (*Informational*)

Date	Region	Event	Impact on OT / Operations
Apr 28, 2025	Europe (Spain/Portugal)	**Iberian Peninsula grid blackout** (not cyber); metros halted; passengers stranded in tunnels; large-scale transport immobilization.	**Severe metro stoppage**; rail service restoration followed grid recovery; raised resilience concerns.
Sep 2025	APAC (Singapore)	**Multiple MRT disruptions** over four days; faults traced to component/signalling/power issues; authority states incidents are isolated, not systemic.	**Line-level slowdowns/halts**; engineering remediation and inspections initiated.

Past 6-Month Snapshot (Apr–Oct 2025)

- **Americas**: One high-impact extortion incident (MTA Maryland) with sustained service friction for vulnerable ridership segments. Rapid public comms and interim call-center workarounds limited passenger risk.
- **Europe**: Non-cyber systemic failure (Iberian blackout) delivered the most acute rail/metro disruption; ongoing grid-stability warnings underscore cross-sector dependency risk to rail OT.
- **APAC**: Elevated nuisance/service disruptions from technical faults; ransomware pressure growing per regional telemetry.

How Land-Transport OT Is Targeted or Fails

- IT→OT spillover (ransomware/extortion) hits dispatch, booking, and traveler-info systems first, forcing degraded ops or manual modes; most events stop short of signaling/ATP compromise.
- Rail RF/control exposure: EoT/HoT linking lacks strong authentication (CVE-2025-1727); feasible command spoofing (emergency brakes) with commodity radios if not mitigated.
- Systemic dependencies: Power/grid instabilities can paralyze metros at scale; comms/power SCADA resilience directly affects rolling stock and wayside availability.

Popular Tactics, Techniques & Procedures (TTPs)

Tactic	ID	Description
Initial Access	T1566	Phishing to foothold in IT, then pivot toward OT jump hosts/engineering assets.
	T0822	External Remote Services (exposed VPN/RDP) for contractor/vendor access abuse into operations domains.
Lateral Movement	T0886	IT–OT lateral movement via shared auth, flat VLANs, or unmanaged jump servers.
Manipulation	T0831	Manipulation of control (e.g., unauthorized brake/stop commands over weak RF links).
Denial	T0813	Denial of control via ransomware on HMI/dispatch or flooding ICS comms.
Inhibit Response	T0838	Disable/impair safety or alarms around wayside/rolling-stock subsystems (precautionary watch).
Collection/Exfil	T1041 / T1486	Data theft for pressure (PII/ops data) alongside encryption (double extortion).

Recommended Controls (prioritized for rail/metro OT)

- Contain IT→OT pathways (now). Enforce hard segmentation/DMZs; broker OT access through jump hosts with MFA; remove direct internet exposure.
- Mitigate EoT/HoT risk. Track CVE-2025-1727; apply vendor firmware/bounds-checking; deploy authenticated/crypto overlays where replacement is pending; restrict RF proximity during operations.
- Ransomware readiness for operations. Offline/immutable backups of dispatch/signaling configs; application allow-listing on HMI/engineering workstations; playbooks for manual train orders and degraded modes.
- OT monitoring tuned for rail. Detect abnormal stop/brake commands, odd schedule changes, new admin accounts, and lateral scans; centralize logs from interlocking servers and traction power SCADA.
- Cross-sector resilience. Coordinate with TSOs/DSOs; simulate loss of power/comms; provision backup comms for control centers (out-of-band radio, sat-links).

- Third-party controls. Tight vendor VPN whitelists; time-bound access; contractual security (IEC 62443 alignment); continuous dark-web/watch for stolen transit data.
- Legacy uplift. Prioritize replacement of unauthenticated RF, obsolete interlockings, and unsupported OS in control rooms; add bump-in-the-wire encryption where replacement lags.
- Human layer. Targeted phishing drills for operations staff; USB/media controls in depots; incident “suspicion to action” guidance for signallers and OCC teams.

Regional Notes (what to watch)

- **Americas**: Expect continued double-extortion against city/transit agencies; protect paratransit/ADA services and traveler-info portals specifically; rehearse mobility service contingencies.
- **Europe**: Grid stability is a rail risk; ensure metro/rail possess black-start-adjacent playbooks and rider evacuation protocols; maintain DDoS cover for public-facing portals as hacktivist noise persists.
- **APAC**: Rising ransomware sophistication and operational fault frequency; close reporting gaps; align with national CI requirements; validate spares/rollback for rolling-stock faults.

Additional Insights

- New rail-specific CVE (CVE-2025-1727) should accelerate a multiyear refresh of rail RF control; monitor vendor SSBs and test-track changes before fleetwide rollouts.
- Law-enforcement pressure on DDoS crews (e.g., NoName057(16) disruption) reduces nuisance but does not reduce ransomware risk; sustain DDoS guardrails.
- Historic precedent (Poland 2023 radio-stop sabotage) shows how low-cost RF abuse can produce high-impact operational halts where authentication is absent.

Reference

[1] Impacts From Cybersecurity Incident (Maryland Transit Administration), https://www.mta.maryland.gov/cybersecurity-incident

[2] Maryland transit data breach claimed by Rhysida (The Record), https://therecord.media/maryland-transit-administration-data-breach-claimed-ransomware-gang

[3] Pittsburgh Regional Transit — Notice of Cyber Incident, https://www.rideprt.org/inside-Pittsburgh-Regional-Transit/notice-of-cyber-incident/

[4] Pittsburgh transit agency victim of ransomware attack (Trains.com), https://www.trains.com/pro/passenger/light-rail/pittsburgh-transit-agency-victim-of-ransomware-attack/

[5] End-of-Train & Head-of-Train Remote Linking Protocol Vulnerability (CISA ICSA-25-191-10), https://www.cisa.gov/news-events/ics-advisories/icsa-25-191-10

[6] CVE-2025-1727 (NVD), https://nvd.nist.gov/vuln/detail/CVE-2025-1727

[7] Major railroad-signaling vulnerability could let hackers stop trains (Cybersecurity Dive), https://www.cybersecuritydive.com/news/railroad-train-vulnerability-derail-brake-cisa-advisory/752940/

[8] The cheap radio hack that disrupted Poland's railway system (WIRED), https://www.wired.com/story/poland-train-radio-stop-attack/

[9] Global operation targets NoName057(16) (Europol), https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network

[10] International operation disrupts NoName057(16) (The Record), https://therecord.media/international-police-takedown-noname-hacker

[11] Spain's grid operator warns of new voltage swings (Reuters), https://www.reuters.com/business/energy/spains-grid-operator-warns-new-tension-swings-urges-measures-avoid-blackout-2025-10-08/

[12] Spain's Red Eléctrica warns of renewed blackout risks (Financial Times), https://www.ft.com/content/b155d922-288a-4bb8-b207-a9f49bb645c7

[13] Personal Data Protection Commissioner investigating Prasarana incident (Malaysia Digital Ministry — Press Release, PDF), https://www.digital.gov.my/api/file/file/5.9.2024_PR_PERSONAL%20DATA%20PROTECTION%20COMMISSIONER%20INVESTIGATING%20RECENT%20CYBERSECURITY%20INCIDENT%20INVOLVING%20PRASARANA%20MALAYSIA%20BERHAD.pdf

[14] Prasarana data breach summary (BreachSense), https://www.breachsense.com/breaches/prasarana-data-breach/