OT-ISAC WHITE *– Recipients may share* ***TLP:WHITE*** *information without restriction.* ***TLP:WHITE*** *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:

Mobile Device and Operational Technology (Healthcare)

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

Hospitals face sustained ransomware and data-extortion pressure, with mobile endpoints (smartphones/tablets, clinician apps, BYOD) routinely used for initial access or credential theft, then leveraged to pivot into converged IT/OT networks (medical devices, labs, BMS/HVAC). In the past year, material disruptions struck the NHS (Synnovis), Kettering Health (US), and KBC Zagreb (Croatia). APAC hospitals report the world's highest weekly attack attempts. Effective defense hinges on hardening mobile/edge access, enforcing Zero Trust segmentation between IT/IoMT/OT, and accelerating device inventory, patching, and OT-aware monitoring.

Key Judgments

Judgment	Detail	Confidence
Ransomware remains the dominant operational risk to hospital OT/clinical operations.	Disruption to labs, imaging, service cancellation across multiple regions, including NA and Europe.	High
Mobile endpoints are frequent entry points.	Though specific mobile-device-entry incidents are less often fully documented, phishing, credential	Medium – High

	theft, and remote service exploits are regularly cited in threat reports (e.g. Interlock warnings).	
APAC hospitals experience the highest attack volume globally.	Multiple vendor & security firm reports show APAC healthcare sees frequent attempted attacks weekly; however, exact comparatives depend on vendor visibility.	High
Converged/flat networks amplify blast radius.	Evidence from Kettering Health: system-wide technology outage, affecting call center, EHR, etc.; shows how one intrusion spreads.	High
Medical device security weaknesses materially affect patient safety.	In the Synnovis case, delays in blood testing due to pathology outage contributed to patient death; shows device/service dependency has safety consequences.	High

Incidents & Trends

Date	Region	Incident & Actor	Impact on OT/Operations
May 20, 2025	North America (USA)	Kettering Health – Interlock ransomware	System-wide outage; call center and scheduling tools affected; elective procedures canceled; emergency operations under strain.
June 3, 2024	Europe (UK)	Synnovis – Qilin ransomware	Pathology services disrupted; blood test delays; thousands of appointments cancelled; patient death linked to delays.
Early to mid-2025	North America / Healthcare sector trend	Rising ransomware operations (Interlock etc.) targeting hospitals	Increased warnings, repeated breach incidents; expansion of double-extortion tactics; more frequent disclosures.

Past 6 months (Mar–Sep 2025) snapshot

Continued NA ransomware (e.g., Kettering recovery period); EU steady high activity; APAC high baseline with frequent probing and smaller breaches, many under-reported. Pattern: double-extortion, third-party/supply chain exposure, infostealer-to-ransomware funnels.

How Mobile Bridges to OT in Hospitals

- Phishing/smishing on clinician devices → credential theft → VPN/RDP reuse; observed in HK campaigns and multiple NA cases.
- Insecure/compromised mobile apps tied to connected devices create MITM/reprogramming risk; FDA has publicly warned on wireless insulin pump risks (excess/insufficient dosing).
- BYOD & shadow IoT expand the trust boundary; unmanaged devices on staff Wi-Fi can scan/pivot into flat segments that include IoMT/OT. APAC volume amplifies exposure.

Popular Tactics, Techniques & Procedures (TTPs)

Tactic	ID	Description
Initial access	T1566	Phishing / Smishing of staff on mobile mail/messaging; MFA gaps exploited.
	T1133	External Remote Services – weak VPN / RDP; purchased access from Initial Access Brokers (IABs).
	T1190	Web / application exploits & file-transfer supply-chain compromises (e.g., MOVEit-style) used to gain footholds and exfiltrate data.
Post-compromise	T1003 / T1078 / T1110 (credential techniques)	Credential dumping & AD abuse; use of valid/stolen accounts; living-off-the-land lateral movement (PsExec, WMI).
	T1046 / T1086 / T1490	Lateral scanning into IoMT/OT on converged VLANs; disabling EDR/AV; targeting backups prior to encryption.
Impact	T1486	Data Encrypted for Impact – ransomware / double-extortion; lab, imaging and pharmacy outages; documented patient harm in EU cases. Data theft / spyware for extortion or espionage; DDoS as adjunct pressure tactic.

Recommended Controls (hospital-specific; prioritized)

- **Mobile Device Management (UEM/MDM) as a gate to data & intranet**
  Enforce device enrollment, OS currency, disk encryption, lockscreen, jailbreak/root detection, remote wipe, per-app VPN, conditional access; containerize hospital apps on BYOD. Block non-compliant devices from email/EHR/VPN.
- **Zero Trust segmentation between IT / IoMT / OT / BMS**
  Separate VLANs; strict ACLs/allow-lists; distinct SSIDs (staff/guest/IoMT); NAC with cert-based admission; micro-seg for PACS/LIS; broker all vendor OT access via MFA'd jump hosts with session recording. Detect east-west anomalies. (Industry best practice aligned to NIS2/HICP.)
- **IoMT/OT asset inventory & vulnerability management**
  Maintain live SBOM-aware inventory; map firmware/OS; monitor CISA/FDA advisories; patch where possible; virtual patching/IPS and isolation for unpatchable legacy devices. Evidence of patient-care impact from device attacks justifies budget.
- **Harden identity & remote access**
  Phishing-resistant MFA (FIDO2) for VPN/RDP & privileged access; just-in-time admin; disable legacy protocols; audit break-glass accounts; geo-velocity & impossible-travel alerts.
- **EDR + OT/IoMT-aware network monitoring**
  Host EDR on IT; passive OT sensors for HL7/DICOM/BACnet baselining and anomaly alerts; block unknown egress from device VLANs.
- **Resilience & response**
  Immutable/offline backups; routine restore tests; downtime/run-on-paper drills with clinical/biomed; parts & spare device plans; ransomware playbooks that include lab/imaging/pharmacy continuity.
- **Secure mobile/clinical apps & web**
  Threat-model companion apps; pin TLS; least-privilege APIs; MAST/DAST pipelines; store secrets in platform keystores; require SSO+MFA.
- **Staff awareness & smishing drills**
  Short, frequent micro-trainings tailored to clinicians and facilities staff; "report-a-phish" in mobile clients.

Regional Notes (what to watch)

- **North America**: Newer crews (e.g., Interlock) adopting classic playbooks; regulator & law-enforcement pressure increasing but operational impact persists. Review vendor and file-transfer exposures.
- **Europe**: Health-sector resilience programs (Action Plan/NIS2) maturing; nevertheless, patient-harm linkage raises liability and duty-of-care stakes – prioritize pathology/lab dependencies.
- **APAC**: Highest attack volume baseline; frequent phishing-led intrusions; ensure Wi-Fi/NAC separation and BYOD governance are not lagging modernization.

Actionable Recommendations

- **Block unmanaged mobile access now**: Conditional access + per-app VPN; quarantine non-MDM devices from email/EHR/VPN.
- **Stand-up an OT/IoMT change freeze window**: Patch highest-risk devices; where not possible, virtually patch + isolate; capture golden configs and back them up offline.
- **Reduce lateral movement blast radius**: Create/verify ACLs that prevent any staff Wi-Fi/office VLAN from initiating connections to PACS/LIS/device VLANs; test with purple-team scans.
- **Harden identity paths**: Enforce phishing-resistant MFA for all remote and admin access; disable legacy auth; rotate service accounts tied to lab/imaging.
- **Telemetry gap-fill**: Deploy passive sensors on device VLANs to baseline DICOM/HL7/BACnet; tune alerts for strange talkers and exfiltration.
- **Exercise downtime playbook quarterly**: Include lab (bloods), imaging, pharmacy; verify manual workflows and spares; rehearse ransomware containment (isolate, triage, restore).

Additional Insights

- **Legal/Regulatory**: In EU, patient-harm linkage (Synnovis) will intensify regulatory scrutiny and civil exposure; align security cases to patient-safety outcomes to unlock budget.
- **Threat Outlook (12 months)**: Expect infostealer – RaaS pipelines and third-party (labs/diagnostics) compromises to remain prime vectors; watch for MDM tenant takeover attempts as identity defenses improve. (Sector inference grounded in recent patterns.)

Reference

[1] Cybersecurity Incident (Kettering Health FAQ), https://ketteringhealth.org/cybersecurity-incident-faq/

[2] Patient Death Linked to Ransomware Attack on Pathology Services Provider (HIPAA Journal), https://www.hipaajournal.com/patient-death-linked-to-ransomware-attack/

[3] Kettering Health Resumes Normal Operations for Key Services Following Ransomware Attack (HIPAA Journal), https://www.hipaajournal.com/kettering-health-ransomware-attack/

[4] World Health Day 2025: When Cyber Security Fails, So Does Public Health, https://blog.checkpoint.com/healthcare/world-health-day-2025-when-cyber-security-fails-so-does-public-health/

[5] HICP, https://405d.hhs.gov/cornerstone/hicp

[6] RunSafe Security Releases 2025 Medical Device Cybersecurity Index Amid Surge in Threats to Patient-Critical Devices, https://runsafesecurity.com/resources/press-releases/2025-medical-device-cybersecurity-index/

[7] LockBit claims cyberattack on Croatia's largest hospital, https://therecord.media/lockbit-claims-cyberattack-croatia-hospital

[8] Ransomware's New Front: Uncovering the Latest Threats Facing Hong Kong, https://www.hkcert.org/blog/ransomware-s-new-front-uncovering-the-latest-threats-facing-hong-kong

[9] FDA reports potential cybersecurity risk with insulin pump system, https://www.aha.org/news/headline/2022-09-20-fda-reports-potential-cybersecurity-risk-insulin-pump-system

[10] Health-ISAC Heartbeat flags surge in ransomware, VPN exploits across healthcare systems, https://industrialcyber.co/medical/health-isac-heartbeat-flags-surge-in-ransomware-vpn-exploits-across-healthcare-systems/

[11] #StopRansomware: Interlock, https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-203a