WIRE Technology & Cyber

UNCLASSIFIED // OPEN SOURCE | Monday, 16 November 2026 | Vol. 2026-320 | As of 160725 EST NOV 26

BLUF. WIRE Technology & Cyber holds at **ENVIRONMENT FOR CRISIS**, trend **=**, with no topic changing level. The 9–15 Nov week closed with **370** ransomware leak-site victims, about 1.48 times the 8-week mean, and **12** KEV additions. Both weekly calls were scored today: TEC-33 (KEV ≥ 10) is a hit and TEC-32 (180–299 victims) is a miss. CoreWeave reported a global outage of its Serverless Inference service on 15 Nov, resolved after about 1.6 hours. Paris prosecutors confirmed a cybercrime probe into the September attack on La Poste subsidiary Maileva, which exposed contact details of 22 million people. South Korea's interior ministry said about 300 government email accounts were breached through a single sign-on flaw. On chips, a senior senator wrote to the Commerce Secretary on 15 Nov urging enforcement against AI-chip flows to China. MOFCOM still has not extended its No. 72 pause, which ends 27 Nov.

0. WIRE Technology & Cyber Dashboard

TOPIC	CRISIS LEVEL	DOM. INDICATOR	KEY DRIVER (today)	TREND
TEC-T1 Critical-infrastructure cyber	ENVIRONMENT FOR CRISIS	SIGNIFICANT	K-3: EFS cold-room attack in window; K-4: 370 leak-site victims, 9–15 Nov	=
TEC-T4 AI governance and incidents	ENVIRONMENT FOR CRISIS	SIGNIFICANT	AI-3: Microsoft 365 outage (12–13 Nov) in window; CoreWeave global inference outage 15 Nov	=
TEC-T3 Space and undersea infrastructure	NO CRISIS	ABNORMAL	O-1: one failed attempt (Lithuania, 18 Oct) in window	=
TEC-T2 Semiconductors and compute	NO CRISIS	ROUTINE	X-1: no new BIS rule; MOFCOM No. 72 pause ends 27 Nov	=

Indicator: ROUTINE | ABNORMAL | SIGNIFICANT | EXTREME **Crisis level:** NO CRISIS | ENV. FOR CRISIS | POTENTIAL | PROBABLE | IMMINENT

Family level = highest topic level. Roll-up per WIRE_METHOD §1a. Trend key: ↑ toward crisis, ↓ away, = no net change.

Change line. No level change. The family stays at ENVIRONMENT FOR CRISIS with trend =.

Moved indicators (vs 15 November). None changed score. K-4 final count for 9–15 Nov rose from 359 to 370 on backfill (still ABNORMAL). K-1 closed the week at 12 (ABNORMAL).

I. TEC-T1 CRITICAL-INFRASTRUCTURE CYBER | ENVIRONMENT FOR CRISIS

Facts. The KEV catalog is still at version **2026.11.13** with **1,781** entries. The 9–15 Nov week closed at **12** additions, and none has been added on 16 Nov so far (KEV feed). Ransomware.live now counts **370** victims for 9–15 Nov (UTC), with 31 on 15 Nov. The mean of the 8 prior weeks (14 Sep–8 Nov) is 249.6 on today's data, so the alert line (1.25 ×) is about 312 (feed). The Paris prosecutor's office confirmed on 15 Nov that its cybercrime unit is investigating a mid-September attack on Maileva, a La Poste group mail platform. Maileva says first names, last names and postal addresses of 22 million people were exposed, and bank details were not (RFI). South Korea's interior ministry said on 16 Nov that hackers entered the government email system through local government networks, using a single sign-on flaw to reach about 300 accounts. It opened a joint probe with the NIS and KISA (Aju Press). Coles told the ASX on 16 Nov that it is investigating a cybersecurity incident and has found no evidence that customer, staff or supplier data was taken (ABC). Monadnock Community Hospital's 15 Nov update says its phones are restored but it remains on downtime procedures, with no timeline for full restoration. The update does not mention ambulance diversion (MCH; WMUR). Vanderbilt's latest update (13 Nov) still calls the event an "ongoing cyberattack". Most systems are back, but OneDrive, SharePoint and Box remain disabled (Vanderbilt). **Indicators.** K-1 ABNORMAL (12, week closed); K-2 ABNORMAL (carried); K-3 SIGNIFICANT (EFS, 2 Nov, in window; Monadnock cause unconfirmed); K-4 ABNORMAL (370, about 1.48 × mean); K-5 ROUTINE. Roll-up: ENVIRONMENT FOR CRISIS. Trend =. **Analyst Comment.** Two weeks in a row above the alert line make it likely (about 65%) that leak-site volume is running at a higher level, not just a one-week spike. Watch TEC-44 for 16–22 Nov. The Maileva case is a reminder that one mail-handling vendor can expose a large share of a country's adults at once.

II. TEC-T4 AI GOVERNANCE AND INCIDENTS | ENVIRONMENT FOR CRISIS

Facts. CoreWeave's status page reported a global outage of Serverless Inference from 20:08 to 21:47 UTC on 15 Nov, with no cause stated (CoreWeave via Rewindex). Amazon's threat intelligence team reports that attackers' AI agents scanned internet-exposed LLM gateways and app builders (LiteLLM, Dify, Langflow and others) to steal and pool AI provider keys. Amazon says it cannot verify the outcomes the agents recorded (The Hacker News). No Fireworks AI statement naming the Cursor key was found (TEC-46 open). The Federal Register API shows no AI-related rule or presidential document since 13 Nov (FR API). **Indicators.** AI-1 ABNORMAL; AI-2 ABNORMAL (Cursor report; key-harvesting campaign); AI-3 SIGNIFICANT (Microsoft 365 outage still in window; CoreWeave short global outage). Roll-up: ENVIRONMENT FOR CRISIS. Trend =. **Analyst Comment.** The Amazon findings and the Cursor case point the same way: AI provider keys are now a target in their own right. Stolen keys pay for the next round of scanning. That makes repeat incidents at AI vendors very likely.

III. TEC-T3 SPACE AND UNDERSEA INFRASTRUCTURE | NO CRISIS

Facts. No new attributed ground-station or cable sabotage was found for 15–16 Nov. The UK government is preparing legislation with prison terms of up to 14 years for deliberate damage to undersea cables and pipelines (Euronews). **Indicators.** O-1/O-2/O-3 ABNORMAL (carried). **Override −1 to NO CRISIS (held):** the only event in the window failed. Trend =.

IV. TEC-T2 SEMICONDUCTORS AND COMPUTE | NO CRISIS

Facts. The Federal Register shows no BIS document since 13 Nov (FR API). The ranking member of the Senate commerce committee wrote to the Commerce Secretary on 15 Nov, saying the department failed to stop advanced AI chips reaching China and urging enforcement under the Export Control Reform Act. The Senate banking committee chair has called the Commerce Secretary to testify in December (CNBC). No MOFCOM notice extending the No. 72 pause on gallium, germanium and antimony exports to the US has been found. The 9 Nov notices extended other pauses to 10 Jan 2027 but did not mention No. 72, which ends 27 Nov (MOFCOM No. 72; Skillings). **Indicators.** X-1–X-4 ROUTINE. Roll-up: NO CRISIS. Trend =. **Analyst Comment.** Pressure from Congress raises the chance of new US licence rules for Southeast Asia (see GAPS and TEC-48). An official rule would move X-1.

V. PREDICTIONS

Resolved: - **TEC-32** (ransomware.live 9–15 Nov total 180–299): **MISS.** The final count is 370. p 0.75, Brier 0.5625. - **TEC-33** (KEV adds ≥ 10 in 9–15 Nov): **HIT.** The count is 12. p 0.35, Brier 0.4225.

Pending: TEC-42 (Monadnock ends diversion by 18 Nov) is open; the 15 Nov update does not mention diversion. TEC-05 and TEC-06 resolve 20 Nov. TEC-09 (MOFCOM No. 72 extension) resolves 27 Nov.

New: - **TEC-47:** Coles Group confirms, between 16 Nov and 15 Dec 2026, that customer, team member or supplier data was accessed or taken in the incident it disclosed on 16 Nov. **30%, unlikely.** - **TEC-48:** BIS publishes a Federal Register rule, between 16 Nov and 31 Dec 2026, that adds a licence requirement for advanced AI chip exports to Malaysia, Indonesia or Singapore. **25%, unlikely.**

VI. GAPS AND UNVERIFIED

- A WSJ report, cited by InvestingLive, says Commerce is drafting licence rules for advanced chip exports to Malaysia, Indonesia and Singapore. It rests on unnamed sources, and no draft rule has been published (InvestingLive).
- Ransomware.live lists Chevron and the University of British Columbia under a group called "ShadowByt3$" on 16 Nov. These are actor claims only and are not confirmed by the organizations.
- Quantum Systems: Der Spiegel reports that other drone makers were also targeted, without details. The payload and attribution remain unconfirmed.
- The cause of CoreWeave's outage is not stated. Monadnock's cause is still unconfirmed.
- GPS jamming in the Baltic is still reported, including a 15 Nov Finnish warning for Helsinki airspace. That warning was seen only in secondary reporting. gpsjam and AIID were not refreshed. Ransomware.live counts use UTC dates and are backfilled.

Sources

CISA KEV; ransomware.live; RFI; Aju Press; ABC News; Monadnock Community Hospital; WMUR; Vanderbilt University; CoreWeave status (Rewindex archive); The Hacker News; Federal Register; Euronews; CNBC; MOFCOM; Skillings; InvestingLive.