WIRE Technology & Cyber

UNCLASSIFIED // OPEN SOURCE | Sunday, 15 November 2026 | Vol. 2026-319 | As of 150722 EST NOV 26

BLUF. WIRE Technology & Cyber holds at **ENVIRONMENT FOR CRISIS**, trend **=**, with no topic changing level. Ransomware.live now lists **359** victims for 9–15 Nov, about 1.34 times the 8-week mean, so the leak-site indicator stays ABNORMAL. Cursor's 13 Nov incident report says an access key exposed by its AI vendor Fireworks led to stolen data and a trojanized Claude Code extension served to up to 5,000 users. Drone maker Quantum Systems confirmed on 12 Nov an "active cyberattack by hostile actors" that preceded a precautionary German flight ban on its drones. The FAA's 13 Nov nationwide ground stop has been tied to a contractor network upgrade, not hacking. No predictions resolved today; TEC-32 and TEC-33 score tomorrow.

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: 359 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; AI-2: Cursor incident report	=
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 14 November). None changed score. K-4 count rose from 323 to 359 (still ABNORMAL). K-1 is unchanged at 12 for the week.

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 count is **12**, and nothing has been added since 13 Nov (KEV feed). The newest directive listed is still ED 26-03 (CISA directives). Ransomware.live counts for 9–15 Nov (UTC) are 100, 67, 36, 99, 19, 18 and 20, a total of **359**. On today's backfilled data, the mean of the 8 prior weeks (14 Sep–8 Nov) is 268.1, which puts the alert line at about 335 (feed). Quantum Systems said on 12 Nov that it found a cybersecurity incident at the end of October and that its investigation "revealed an active cyberattack by hostile actors." Reporting says a malicious update for its QBase ground software reached customer systems, and the German forces grounded the company's drones from 6 Nov as a precaution. The Bamberg cybercrime prosecutors are investigating against unknown persons (BreachNews). Monadnock Community Hospital's latest update (13 Nov) still lists ambulance diversion and downtime procedures through 18 Nov (MCH; WMUR). N-able (11 Nov) says it has fixed every N-central flaw that an unauthenticated user could exploit, and that it has seen no compromise of its hosted servers (N-able). Not cyber: the FAA's 13 Nov nationwide ground stop lasted more than four hours. The Transportation Secretary tied it to contractor upgrade work on the air-traffic telecom network, and officials report no sign of hacking (CNBC; SecurityWeek). **Indicators.** K-1 ABNORMAL (12); K-2 ABNORMAL (carried); K-3 SIGNIFICANT (EFS, 2 Nov, in window; FAA outage not cyber, Monadnock cause unconfirmed); K-4 ABNORMAL (359, about 1.34 × mean); K-5 ROUTINE. Roll-up: ENVIRONMENT FOR CRISIS. Trend =. **Analyst Comment.** The Quantum Systems case is a hijacked update channel at a supplier to Ukraine. It is likely to raise pressure on European defense suppliers to vet their update chains. The FAA event did not come from an attack, but it shows that one faulty network change can halt US aviation for hours. That is the same failure mode an attacker would aim for.

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

Facts. Cursor's incident report (13 Nov) says an attacker used an access key that Cursor had issued to Fireworks, which Fireworks then exposed, to copy coding-agent traces. Some traces held unredacted credentials, which let the attacker into SaaS tools. A stolen credential was then used to put malicious copies of the Claude Code extension (2.1.312 and 2.1.313) on Cursor's marketplace cache on 29 Oct for about 11 hours, and up to 5,000 users may have received them. Cursor says the last attacker activity was on 1 Nov and that it has moved all inference off Fireworks (Cursor). BleepingComputer links the case to a wider wave of attacks on AI developer platforms (BleepingComputer). Microsoft's status feed shows its consumer services operational as of 12:21 UTC on 15 Nov (Microsoft 365 status). **Indicators.** AI-1 ABNORMAL; AI-2 ABNORMAL (Cursor incident report); AI-3 SIGNIFICANT (Microsoft 365 outage still in window). Roll-up: ENVIRONMENT FOR CRISIS. Trend =. **Analyst Comment.** The Cursor case shows that training-data traces can carry live secrets. This is very likely a repeatable weakness wherever AI vendors share data, rather than a one-off. TEC-T4 is likely to step down once the Microsoft outage leaves the window.

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

Facts. No new attributed ground-station or cable sabotage was found for 14–15 Nov. Cirion reports a shunt fault, found 10 Nov, on the Panama–St. Croix subsea cable. It gave no hostile cause (Cirion). **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. No BIS document has been published since 13 Nov (FR API). No MOFCOM notice extending the No. 72 pause on gallium, germanium and antimony has been found; the pause ends 27 Nov (MOFCOM No. 72). **Indicators.** X-1–X-4 ROUTINE. Roll-up: NO CRISIS. Trend =.

V. PREDICTIONS

Resolved: none today.

Pending: TEC-33 (KEV ≥ 10, 9–15 Nov) is at 12 and TEC-32 (180–299 victims) is at 359. Both score on 16 Nov. TEC-42 (Monadnock ends ambulance diversion by 18 Nov) is still open, and the hospital's latest update still lists diversion.

New: - **TEC-45:** A German federal body publicly names Russia, a Russian state agency or a named Russia-linked group as responsible for the Quantum Systems cyberattack by 31 Dec 2026. **20%, unlikely.** - **TEC-46:** Fireworks AI publicly acknowledges, between 15 and 30 Nov 2026, that the Cursor-issued key or Cursor data it held was exposed. **30%, unlikely.**

VI. GAPS AND UNVERIFIED

- Quantum Systems: the reach of the malicious update, the malware's purpose and the attribution to Russia all come from unnamed sources. No official has confirmed them.
- Ransomware.live lists major brands (for example Starbucks, Gap and Samsung) under a group called "N0n" on 14 Nov. These are actor claims only and are not confirmed by the companies.
- Microsoft's preliminary root cause is known only through secondary reporting. No post-incident review has been read directly.
- The FAA's cause comes from an official briefing reported by the press. The FBI's review is not final.
- The causes at Monadnock and Vanderbilt are unconfirmed, and Vanderbilt has not confirmed data theft. gpsjam and AIID were not refreshed. Ransomware.live counts use UTC dates and are backfilled.

Sources

CISA KEV and directives; ransomware.live; BreachNews; Monadnock Community Hospital; WMUR; N-able; CNBC; SecurityWeek; Cursor; BleepingComputer; Microsoft 365 status; Cirion Technologies; Federal Register; MOFCOM.