FENESTRA TI

GLOBAL INTELLIGENCE. CONNECTED INSIGHT.

THREAT LANDSCAPE

August 2026

Ransomware, cyber intelligence, dark web activity, and physical/geospatial security — a monthly view of the threats that actually moved this month.

EXECUTIVE SUMMARY

THE MONTH AT A GLANCE

August's ransomware leadership continues to diverge sharply from the names still dominating mainstream coverage, and the cyber threat landscape was defined less by a single actor than by a small cluster of internet-facing platforms — VPN gateways, Git servers, collaboration software, print management — that both state-sponsored and criminal actors are hitting in parallel.

Several of August's findings point to actors worth a dedicated deeper look, flagged at the end of this report.

25.9%
US share of global physical/conflict activity — no other country tracks above 9%

~32%
Share of named ransomware victims from just three groups

5
Edge-infrastructure vendors shared by state and criminal actors

GEOSPATIAL & PHYSICAL SECURITY ACTIVITY

WHERE ACTIVITY CONCENTRATED IN AUGUST

8.9%

India's share of global activity

A notable presence in this month's global top tier, driven largely by activism and public disorder activity

By category: violence (20.5%) and conflict (18.9%) together account for roughly two-fifths of tagged activity, with activism (18.2%) close behind as a genuine third pillar rather than a residual category. Crime (15.7%) and terrorism (12.2%) follow, with environmental (9.7%), public disorder (2.9%), and cyber (1.9%) rounding out the picture. Events can carry more than one category, so shares don't sum to 100%.

By country: the US leads by a wide margin (25.9%), with India (8.9%), Ukraine (4.5%), the UK (4.4%), Pakistan (4.3%), Israel (3.9%), the Palestinian Territories (3.4%), Russia (2.8%), Nigeria (2.6%), and Iran (2.2%) forming the rest of the top tier.

MARITIME & AVIATION SECURITY

PERSISTENT PRESSURE, TWO LIVE CORRIDORS

The Strait of Hormuz / Gulf of Oman corridor remained a live flashpoint through August: a projectile struck and damaged the engine room of a tanker off Oman (reported via UKMTO), Yemeni forces reportedly forced multiple Saudi-flagged tankers to reroute, and Iranian officials publicly threatened to further restrict Hormuz transit if US naval posture in the area continued — all despite an active US/allied naval presence, underscoring that presence alone isn't fully deterring disruption in one of the world's most consequential shipping corridors.

European airspace saw a genuine escalation, not just continued incursions: a Spanish F-18 shot down a drone that breached Romanian airspace via Moldova in mid-August — the first live intercept we noted this month, versus the usual pattern of unaddressed incursions. Romania's own reporting put 2026 incursions at nearly triple 2025's total. Moldova separately saw a multi-drone incursion event days before its Independence Day parade. Separately, a Polish F-16 intercepted a Russian Il-20 aircraft over the Baltic Sea.

Worth watching as a secondary, less-established flashpoint: China conducted naval and air patrols and drills around a disputed shoal near the Philippines in the South China Sea during August — a different theatre than the above, but one to track for escalation in future editions.

RANSOMWARE

THE REAL LEADERBOARD DOESN'T MATCH THE HEADLINES

The names generic press coverage still leans on — LockBit, BlackCat, ALPHV — don't crack the real top tier this month. Qilin, TheGentlemen, and Clop lead, together accounting for ~32% of all named August victims. The US remains the single most-targeted country (~34% of victims), with the remainder spread thinly across dozens of other countries.

By sector: Manufacturing leads (~15%), followed by Technology (~13%), Professional Services (~11%), and Healthcare (~10%).

NOTABLE EXPLOITED CVES / TARGETED SYSTEMS

CVE-2026-8452 — CITRIX NETSCALER ADC/GATEWAY RCE

Added to CISA's Known Exploited Vulnerabilities catalog; confirmed under active mass ("pray and spray") exploitation. Over 22,000 NetScaler instances remain exposed publicly.

CVE-2026-60004 — GITEA SELF-HOSTED GIT SERVER — CODE INJECTION

Actively exploited; CISA gave federal agencies a 3-day patch window.

CVE-2026-55040 / CVE-2026-63520 — MICROSOFT SHAREPOINT — CHAINED AUTH-BYPASS + RCE

Publicly weaponised within a day of PoC release and actively probed against exposed servers.

PAPERCUT NG/MF — PRINT-MANAGEMENT SOFTWARE — ZERO-DAY

Active zero-day exploitation against internet-exposed servers; vendor issued an emergency out-of-band patch.

The common thread is internet-facing edge/perimeter software rather than any single vendor or sector — consistent with Clop's own historical playbook of mass-exploiting one platform vulnerability across many victims at once rather than bespoke, one-by-one intrusions.

CYBER THREAT INTELLIGENCE

THE SAME HANDFUL OF PLATFORMS, TWO KINDS OF ADVERSARY

DARK WEB / UNDERGROUND FORUMS

Nothing rose above background noise this month. Forum-side activity was dominated by recycled, generic exploit-kit and crypter advertising rather than credible new zero-day trade or breach chatter worth flagging.

CYBER INTEL

The standout finding this month is a joint industry analysis (Tenable/SentinelOne) that quantifies something worth acting on directly — state-sponsored and financially-motivated (ransomware) actors are independently converging on the same narrow set of edge-infrastructure vendors: F5, Citrix, Ivanti, Check Point, and Fortinet.

~54%
of F5 customer environments carry at least one exposed, actively-exploited CVE

461 days
median time-to-patch for Citrix customers — slowest of the group

For any organisation running these platforms, patch cadence on them specifically is currently one of the highest-leverage defensive actions available.

August's Patch Tuesday also underscored scale: Microsoft alone shipped fixes for 415 CVEs (62 rated critical), including one already under zero-day exploitation before the patch shipped. The same edge-platform CVEs named in the Ransomware section — Citrix, SharePoint, Gitea, PaperCut — are the direct connective tissue between that section and this one: the same handful of platforms are driving both ransomware initial access and broader cyber intel reporting this month.

THREAT ACTOR SPOTLIGHT

CLOP (TA505) — RIDING THE EDGE-SOFTWARE WAVE

WHO THEY ARE

A financially-motivated extortion operation (aka Cl0p), active since 2019 and linked to the TA505 collective — already in our registry as known for exploiting zero-days in managed file-transfer and similar platforms, prioritising data theft over encryption.

WHAT OUR OWN AUGUST DATA SHOWS

Clop's presence in Fenestra's ransomware feed is heavily concentrated in August, with a pronounced skew toward Technology-sector victims — consistent with mass-exploiting a single vulnerability across many organisations at once, rather than one-by-one intrusions.

THE HISTORICAL PATTERN, CONFIRMED IN OUR OWN DATA

A real April 2023 case in our cyber-reporting archive shows this exact dynamic before — LockBit and Clop both exploited a critical PaperCut vulnerability chain, and weeks later Microsoft revealed Iranian state-linked groups Muddywater and APT35 had piggybacked on the same flaw. A documented, concrete instance of the "criminal and state actors converge on the same platform" pattern described in this month's cyber intel section.

WHY THAT MATTERS RIGHT NOW

PaperCut is back in the headlines — a brand-new zero-day pair (CVE-2026-81578 / CVE-2026-82078) has been under active exploitation for data theft since August 29. Public reporting hasn't attributed the current campaign to a specific actor yet, but the technique (auth-bypass into data exfiltration, not encryption) matches Clop's documented M.O. closely enough to be worth watching.

RECOMMENDATION

Treat this as live regardless of eventual attribution — prioritise PaperCut's emergency patches (and the other edge platforms named earlier: Citrix NetScaler, Gitea, SharePoint) on any internet-exposed instance now.

Caveat: this draws a pattern parallel, not an attribution claim — the current PaperCut campaign is still publicly unattributed.

THREAT ACTOR SPOTLIGHT

ANSAR ALLAH (THE HOUTHIS) — ESCALATION BEYOND YEMEN

83 **Houthi-linked mentions in Fenestra's Global Events data this month**
Second only to Hamas among the non-state armed groups Fenestra tracks — and far ahead of any other

WHO THEY ARE

Ansar Allah (commonly "the Houthis"), an Iran-aligned movement controlling much of northern Yemen — already in our registry as a non-state armed group with a documented history of cross-border missile/drone strikes and Red Sea shipping attacks.

WHAT OUR OWN AUGUST DATA SHOWS

The 2022 truce with the Yemeni government read as unravelling in real time this month: direct ground clashes on the Taiz front lines, a claimed drone strike on Saudi Aramco's Jizan refinery, and a real resumption of Red Sea shipping attacks — including a strike on an Egyptian-owned cargo vessel that killed four crew (later revised to six) and a claimed attack on the Saudi-flagged tanker Wafa off Yanbu. Real reporting in our own data traces the current escalation to a specific trigger — a Saudi airstrike on July 13 — with the UN separately warning Yemen is at its highest risk of renewed major conflict since the truce began.

WHY IT CONNECTS BEYOND YEMEN

This isn't an isolated theatre. Houthi attacks on Red Sea and Bab el-Mandeb shipping directly complement the Strait of Hormuz pressure covered in this edition's Maritime & Aviation section — two of the world's most consequential shipping corridors under strain at once, from different but adjacent actors. Our own data also links the two more directly: reporting this month explicitly ties a resurgence in Somali piracy to regional naval forces being stretched thin by the wider Iran-linked conflict — a real second-order effect of the same regional pressure, not a separate story.

RECOMMENDATION

For any organisation with Red Sea, Gulf of Aden, or southern Saudi exposure — shipping, energy, logistics — treat this as an active, escalating threat rather than background risk, and track routing advisories in real time given the pace of named vessel and facility attacks this month.

Caveat: incident attribution above reflects Houthi/Ansar Allah's own public claims and government/press reporting as captured in our data — independent verification of responsibility for individual attacks varies.

contact@fenestra-ti.com