INTRUVENT TECHNOLOGIES
Threat Intelligence & Advisory

Generated: December 01, 2025

BRACE THREAT INTELLIGENCE

Cross-Sector Threat Intelligence Report

November 2025 | 16 Critical Infrastructure Sectors Analyzed

39	79	74	80	54%	48m
THREAT ACTORS TRACKED	CONFIRMED INCIDENTS	CVES EXPLOITED	EMERGING SIGNALS	RUSSIAN ATTRIBUTION	AVG BREAKOUT TIME

*All statistics and intelligence sourced from BRACE Threat Intelligence Platform unless otherwise noted with **

01

THREAT LANDSCAPE OVERVIEW

Global Threat Summary — November 2025

Cyberattacks continue to escalate across all critical infrastructure sectors. In November 2025, threat actors demonstrated sophisticated tactics targeting 16 sectors, with ransomware groups and nation-state actors dominating the landscape.

THREAT PULSE

Percentage of sectors experiencing each threat type this month

1. Ransomware — 81%
   - 13/16 sectors
2. Nation-State — 63%
   - 10/16 sectors
3. Supply Chain — 44%
   - 7/16 sectors
4. Hacktivism — 25%
   - 4/16 sectors

02

THREAT ACTOR ANALYSIS

Top Actors & Attribution — November 2025

TOP 5 THREAT ACTORS — SECTOR SPREAD

	Actor	Origin	Sectors
1	Akira Ransomware	Russia	13 sectors
2	Qilin Ransomware	Russia	8 sectors
3	Volt Typhoon	China	8 sectors
4	Clop Ransomware	Russia	6 sectors
5	LockBit 3.0	Russia	6 sectors

THREAT ATTRIBUTION

Russia	54%	China	16%
Unknown	18%	Iran	4%

THREAT OF THE MONTH

Akira Ransomware

"The Sector Saturator"

Akira has emerged as the most pervasive ransomware group, successfully compromising organizations across nearly every critical infrastructure sector. Their sophisticated double-extortion tactics and aggressive affiliate network have generated over $244M in ransom payments. Security teams should prioritize patching VPN appliances and implementing MFA, as these are Akira's primary entry vectors.

13/16 sectors targeted (81%)

03

SECTOR RISK & TTP CONVERGENCE

ITR Scores & Attack Patterns Across 16 Sectors

INTRUVENT THREAT RATING: TOP 10 SECTORS

Higher score = higher threat | % = Month-over-Month change

Sector	Score	Change
Nuclear Reactors	81.7	+24%
Dams	80.5	+15%
Gov. Services	79.6	+16%
Defense Ind. Base	76.2	+19%
Chemical	75.5	+8%
Water/Waste.	72.3	+10%
Emergency Svc.	67.5	+9%
Transportation	66.9	+2%
Info. Tech.	66.5	+9%
Healthcare	64.3	+4%

UNIVERSAL ATTACK CHAIN

Most common TTP sequence observed across all sectors

TTP COVERAGE HEATMAP

TTP presence by sector (darker = more actors using technique)

Sector	T1078	T1486	T1190	T1021	T1490	T1567	T1059	T1133
Commercial	●	●	●	●	●	●	●	●
Communications	●	●	●	●	●	○	●	●
Critical Mfg	●	●	●	●	●	●	●	●
Dams	●	●	●	●	●	○	●	●
Defense Ind.	●	●	●	●	○	●	●	○
Emergency Svc	●	●	●	●	●	●	◐	●

KEY INSIGHT

T1078 (Valid Accounts) is present in ALL 16 sectors with 32 actors using it. Focus defensive investments on credential security — MFA, privileged access management, and credential monitoring should be top priorities.

04

CVEs & INCIDENT INTELLIGENCE

79 Incidents Across 16 Sectors

"MOST WANTED" — TOP THREAT ACTORS

Akira Ransomware
"The Sector Saturator"
Russia
$244M in ransoms
13/16 sectors (81%)

Qilin Ransomware
"The RaaS Absorber"
Russia
+280% attacks YoY
8/16 sectors (50%)

Volt Typhoon
"Living-off-the-Land"
China
8 sectors infiltrated
8/16 sectors (50%)

EMERGING SIGNAL — HIGH CONFIDENCE

Ransomware Cartel Formation: LockBit 3.0, Qilin, and DragonForce have formed a coordinated cartel following RansomHub's collapse in April 2025. This consolidation increases attack sophistication and affiliate reach across critical infrastructure sectors.

CVE SEVERITY DISTRIBUTION (74 CVEs)

- CRITICAL: 28 (38%)
- HIGH: 35 (47%)
- MEDIUM: 11 (15%)

Top CVEs: CVE-2024-40766 (9.3), CVE-2024-3400 (10.0), CVE-2024-21887 (9.1)

ITR SCORE BREAKDOWN: CROSS-SECTOR AVERAGES

Average dimension scores across all monitored sectors

24.8	18.9	7.3	9.7	60.8
of 40 pts	of 25 pts	of 20 pts	of 15 pts	of 100 pts
THREAT ACTOR PRESSURE	VULN EXPOSURE	ATTACK SUCCESS	SOPHISTICATION	OVERALL ITR

05

EMERGING SIGNALS & EXECUTIVE ACTIONS

80 Early Warning Indicators Identified

EMERGING THREAT SIGNALS

13 OT/ICS Threats	12 AI-Enabled Attacks	10 Ransomware Evolution
10 Nation-State Prepos	6 Supply Chain Risk	2 Social Engineering

TREND INDICATORS

Malware Emails YoY*	▲ +131%
Supply Chain Breaches*	97% orgs
OT Patch Delay vs IT*	6x slower
Phishing Attacks YoY*	▲ +21%
Shadow AI Risk (2030)*	40% orgs

THREE THINGS TO KNOW

1
AKIRA IS EVERYWHERE
13/16 sectors (81%)
$244M in ransoms

2
CHINA IS EXPANDING
8 sectors pre-positioned
Volt Typhoon active

3
CREDENTIALS ARE KEY
16/16 sectors
T1078 in ALL sectors

QUICK WINS — DO THIS NOW

- [ ] Enable MFA on VPNs (SonicWall, Ivanti, Fortinet)
- [ ] Patch CVE-2024-40766, CVE-2024-21887, CVE-2024-3400
- [ ] Audit third-party/vendor access
- [ ] Review OT/IT network segmentation
- [ ] Test backup restoration procedures

SOURCES

BRACE Threat Intelligence — Sector research & ITR scores
Hornetsecurity — Cybersecurity Report 2026
BlueVoyant — Supply Chain Defense Report (Nov 2025)
Trellix — OT Threat Report (Nov 2025)
Gartner — GenAI Blind Spots Report (Nov 2025)
CrowdStrike — Global Threat Report 2025