



BRACE THREAT INTELLIGENCE

# Cross-Sector Threat Intelligence Report

November 2025 | 16 Critical Infrastructure Sectors Analyzed

39

THREAT ACTORS TRACKED

79

CONFIRMED INCIDENTS

74

CVES EXPLOITED

80

EMERGING SIGNALS

54%

RUSSIAN ATTRIBUTION

48m

AVG BREAKOUT TIME

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

## 01

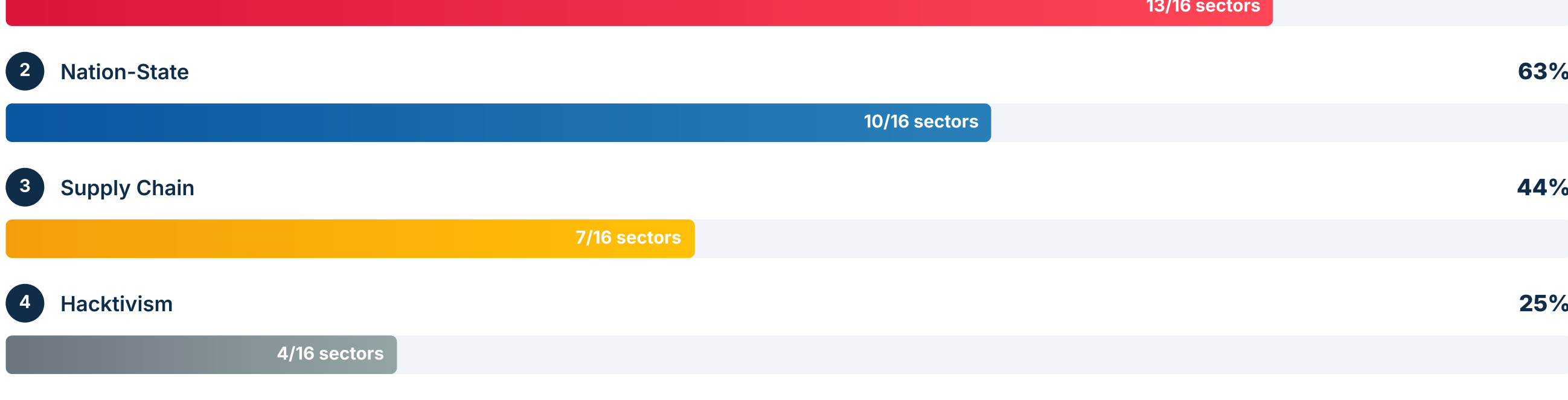
### THREAT LANDSCAPE OVERVIEW

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

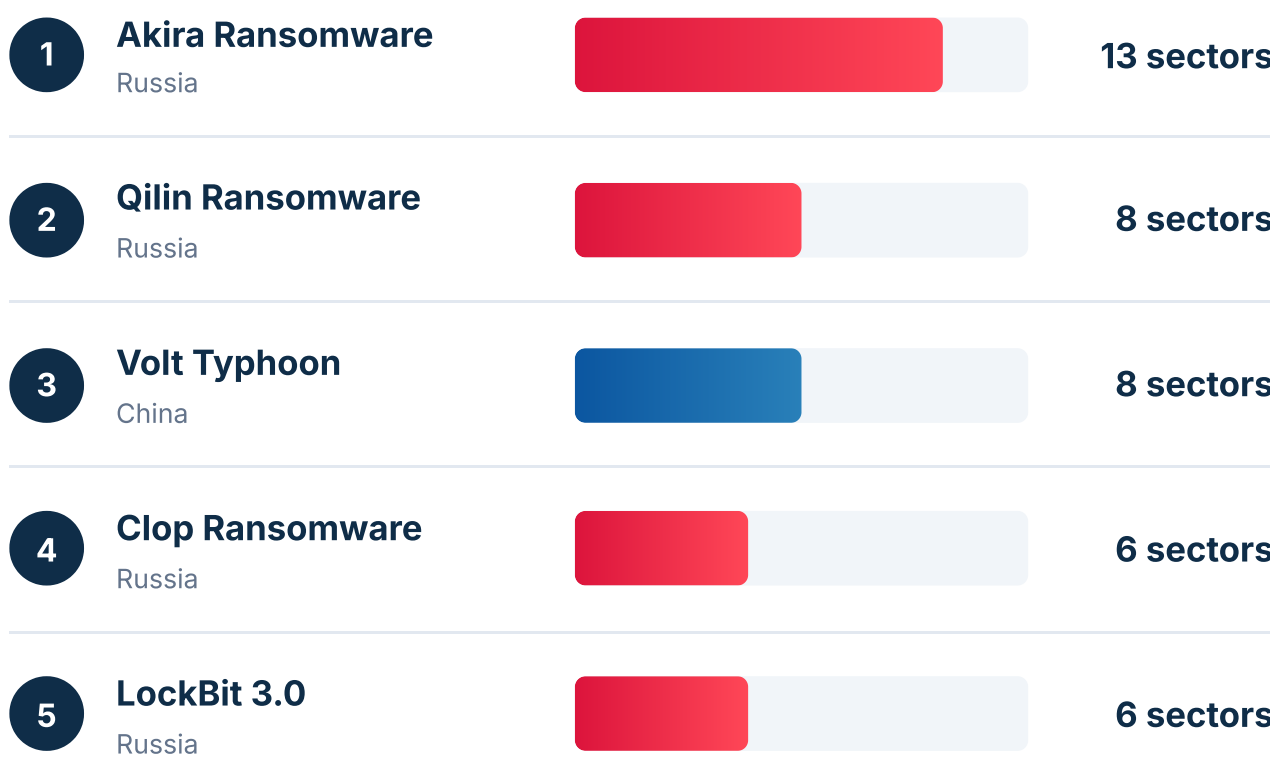


## 02

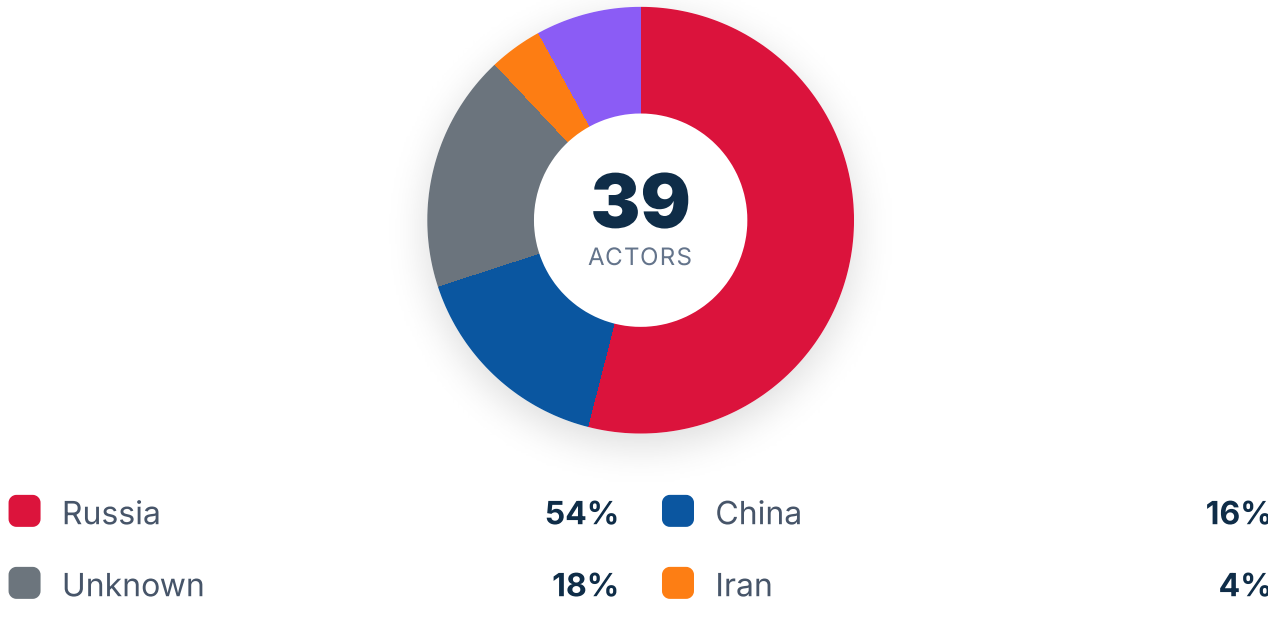
### THREAT ACTOR ANALYSIS

Top Actors & Attribution — November 2025

#### TOP 5 THREAT ACTORS — SECTOR SPREAD



#### THREAT ATTRIBUTION



#### 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%)

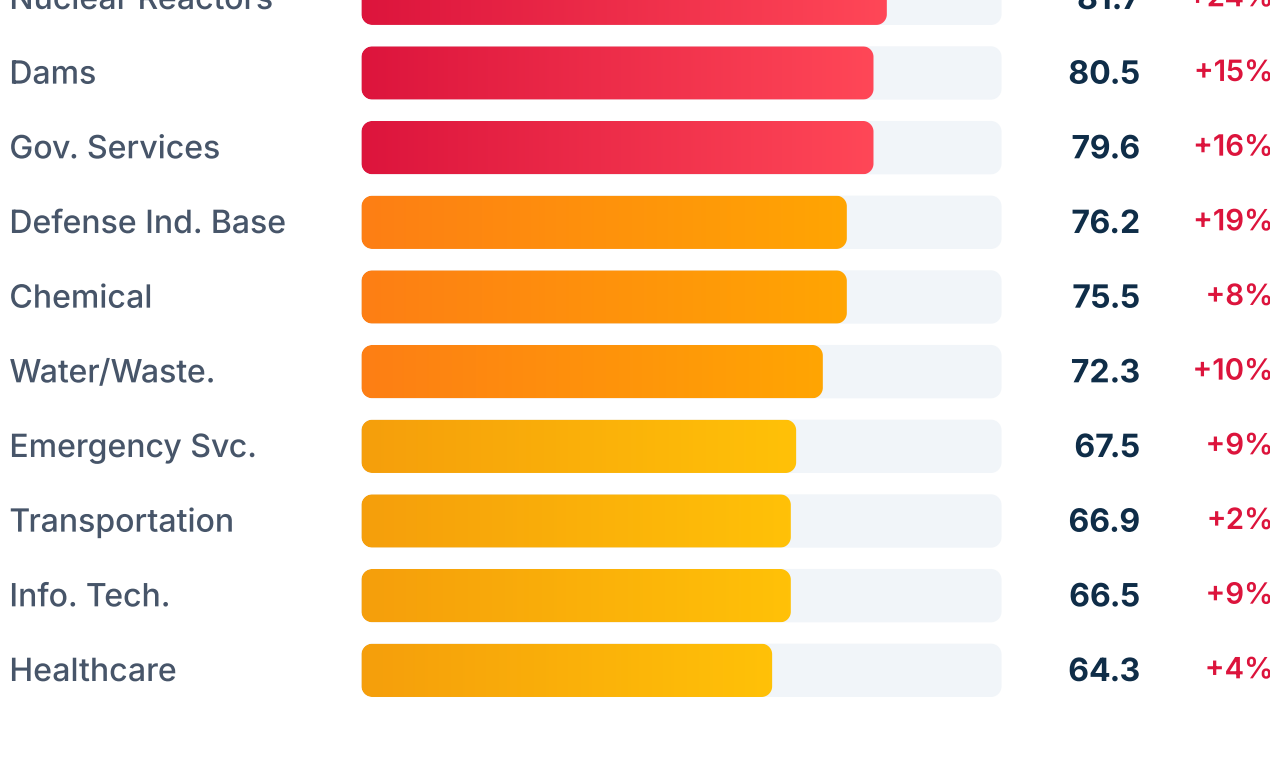
## 03

### SECTOR RISK & TTP CONVERGENCE

ITR Scores & Attack Patterns Across 16 Sectors

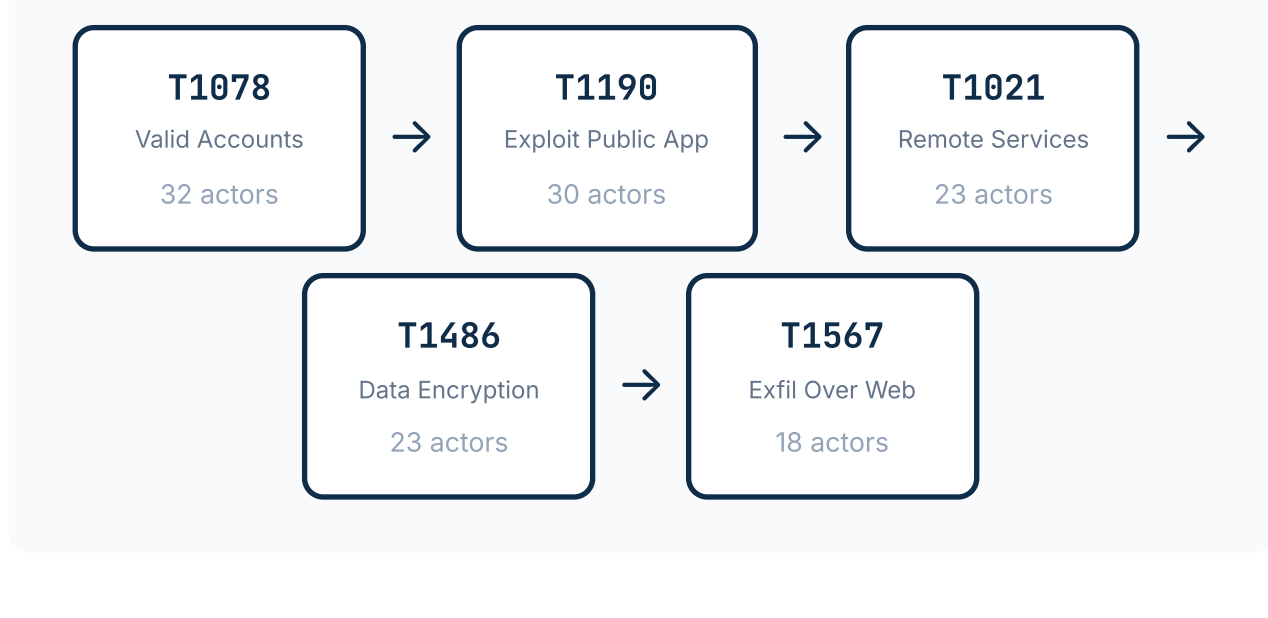
#### INTRUVENT THREAT RATING: TOP 10 SECTORS

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



#### 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

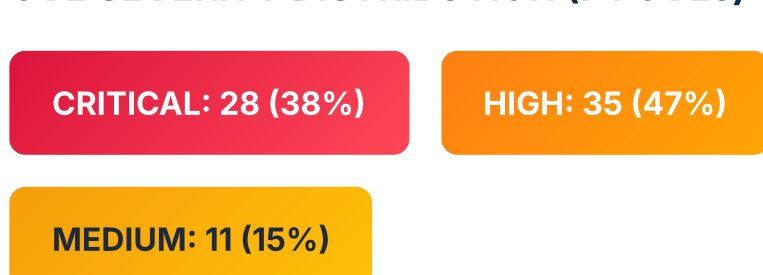


#### EMERGING SIGNAL

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)



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

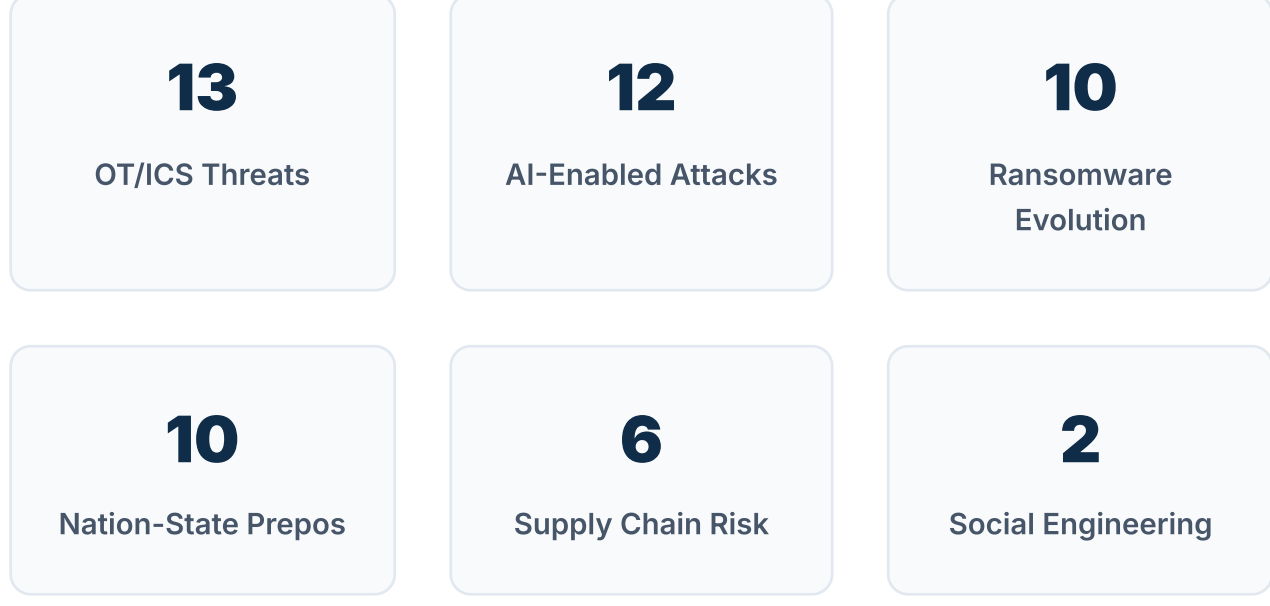


## 05

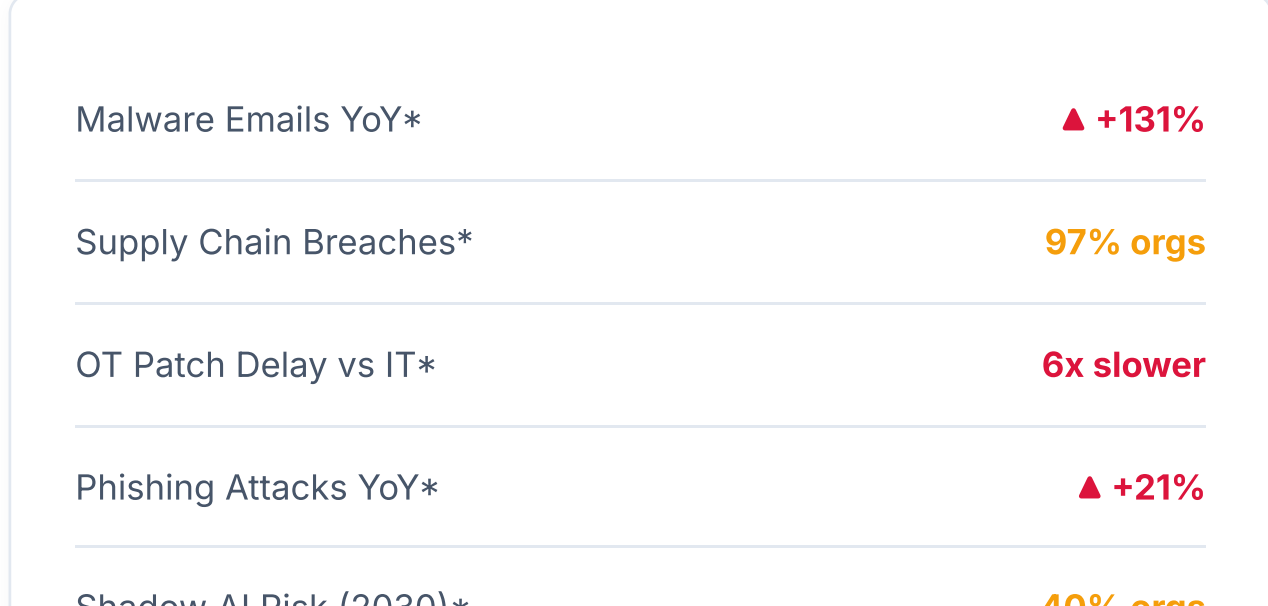
### EMERGING SIGNALS & EXECUTIVE ACTIONS

80 Early Warning Indicators Identified

#### EMERGING THREAT SIGNALS



#### TREND INDICATORS



#### THREE THINGS TO KNOW



#### 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 | Trellix — OT Threat Report (Nov 2025)  
Hornetsecurity — Cybersecurity Report 2026 | Gartner — GenAI Blind Spots Report (Nov 2025)  
BlueVoyant — Supply Chain Defense Report (Nov 2025) | CrowdStrike — Global Threat Report 2025