

MONTHLY INTELLIGENCE BRIEF

Cross-Sector Threat Intelligence

December 2025 | 16 Critical Infrastructure Sectors Analyzed

59 THREAT ACTORS TRACKED

81 CONFIRMED INCIDENTS

46 CVEs EXPLOITED

82 EMERGING SIGNALS

All statistics sourced from BRACE Threat Intelligence Platform unless otherwise noted

01 EXECUTIVE PULSE

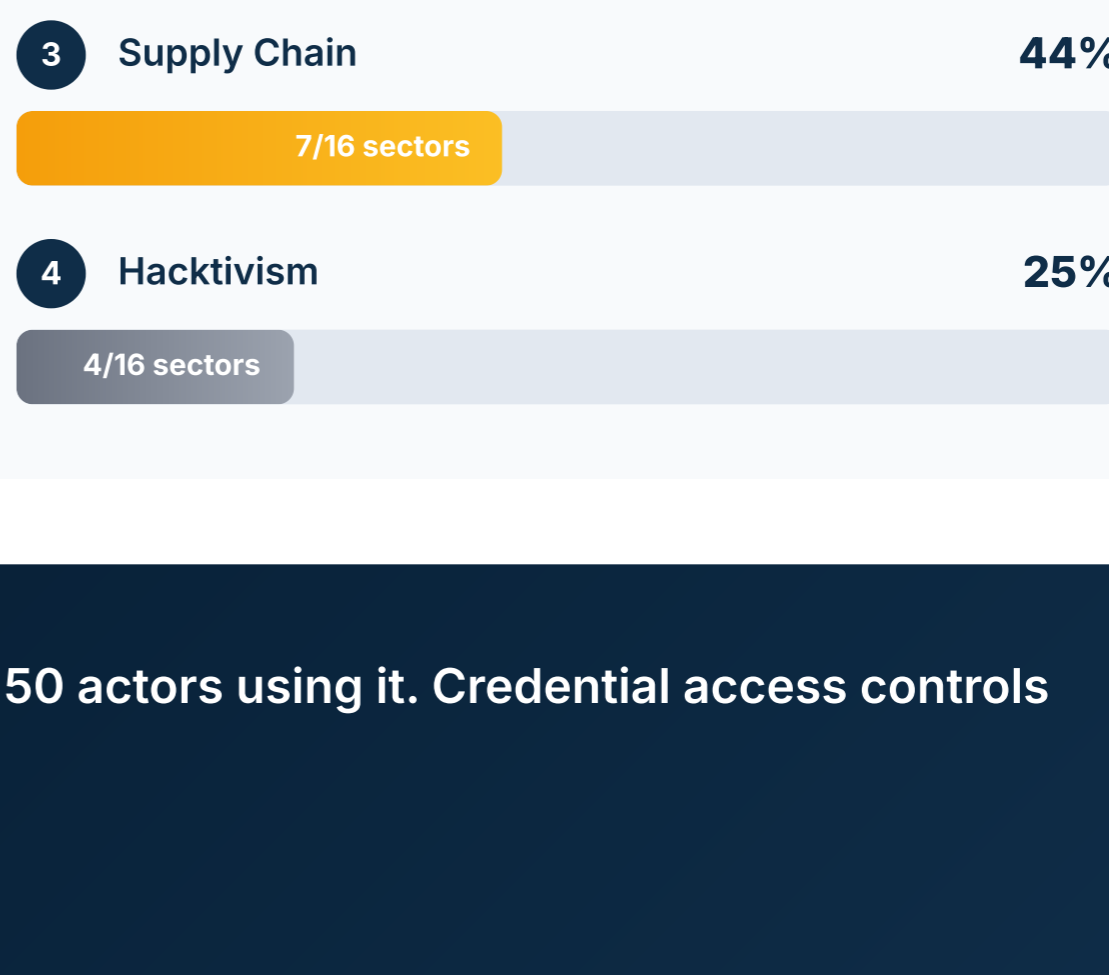
Global Threat Summary — December 2025

48min AVERAGE ECRIME BREAKOUT TIME

Down from 62 minutes in 2024. Breakout time measures how quickly attackers move from initial compromise to lateral movement across your network—leaving defenders less time to respond.

THREAT PULSE

Percentage of sectors experiencing each threat type



T1078 (Valid Accounts) is present in ALL 16 sectors with 50 actors using it. Credential access controls remain foundational to any effective security posture.

— BRACE Threat Intelligence Analysis

02 INTELLIGENCE NARRATIVES

Three Stories Defining December's Threat Landscape

Salt Typhoon: The Telecom Compromise That Won't End

In December 2025, Senate Commerce Committee experts delivered an uncomfortable verdict: nine major US telecommunications carriers, including Verizon, AT&T, and T-Mobile, have failed to prove Chinese hackers have been eradicated from their networks.

Salt Typhoon's persistence is a demonstration of capability, not a failure of detection. The group has maintained access through multiple detection attempts, credential rotations, and infrastructure changes. They're proving they can stay as long as they want.

Why this matters: Telecom infrastructure carries more than calls. Authentication systems, SMS-based MFA, and carrier-trusted certificates all flow through networks that remain compromised. If you're relying on telecom-based security controls, it's time to reassess those trust assumptions.

Volt Typhoon's Quiet Expansion: 10 Sectors and Counting

Volt Typhoon expanded from 8 sectors in November to 10 in December, adding Information Technology and Transportation Systems. The McCrary Institute's "Code Red" report documented access maintained for over 300 days in some electric grid environments.

The pattern stays consistent: no custom malware, no obvious indicators, just valid credentials and native system tools. They're playing the long game, establishing positions that would matter if competition becomes conflict.

Why this matters: Traditional IOC-based detection won't find Volt Typhoon. They use your tools, your credentials, your pathways. Finding them requires behavioral baselines and anomaly identification that most organizations haven't implemented yet.

Ivanti: Ground Zero for Chinese APT Initial Access

Two critical Ivanti Connect Secure vulnerabilities (CVE-2025-0282 and CVE-2025-22457) have become the go-to initial access vector for Chinese nation-state actors. UNC5221, the same group behind Volt Typhoon activity, exploited CVE-2025-0282 as a zero-day in late December 2024, deploying SPAWN malware before patches were available.

By April 2025, CVE-2025-22457 followed the same playbook: China-nexus actors deploying TRAILBLAZE and BRUSHFIRE malware against the VPN infrastructure that organizations depend on for secure remote access.

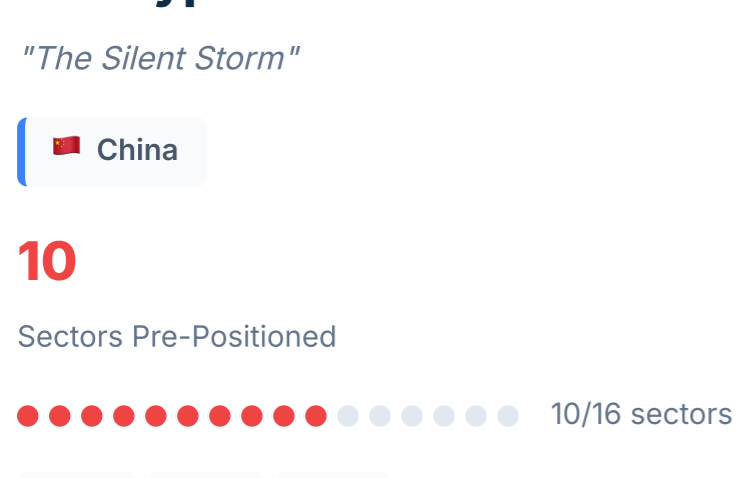
Why this matters: If your organization runs Ivanti Connect Secure, assume you've been scanned. Verify patch status immediately. Patching alone won't cut it though. You need forensic review for indicators of prior compromise. The attackers had weeks of head start.

03 THREAT ACTOR SPOTLIGHT

Top Actors & Attribution — December 2025

"MOST WANTED" — TOP THREAT ACTORS

ACTIVE THREATS



Volt Typhoon

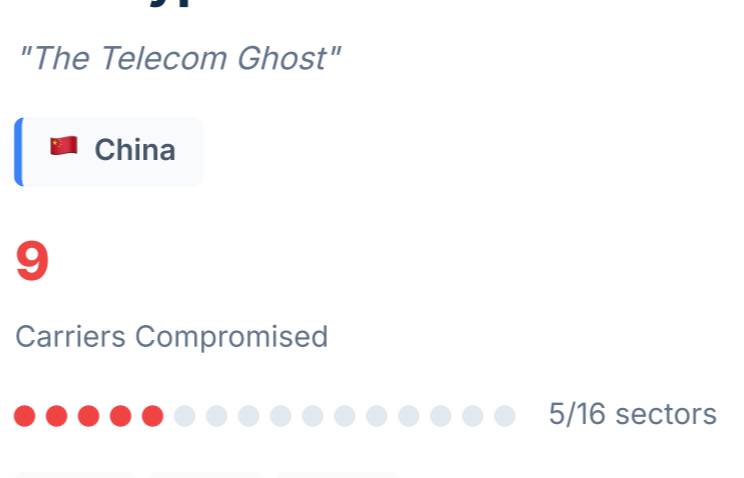
"The Silent Storm"

China

10 Sectors Pre-Positioned



T1078 T1071 T1021



Salt Typhoon

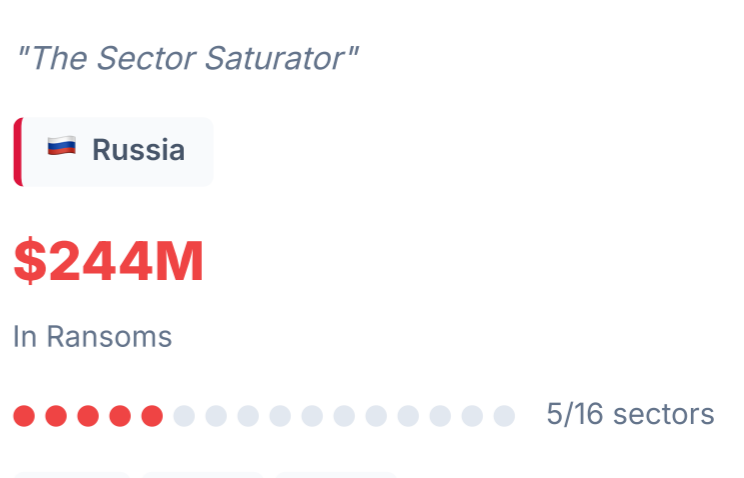
"The Telecom Ghost"

China

9 Carriers Compromised



T1078 T1557 T1040



Akira

"The Sector Saturator"

Russia

\$244M In Ransoms



T1190 T1059 T1486

THREAT OF THE MONTH



Salt Typhoon

"The Telecom Ghost"

Chinese state-sponsored actor maintaining persistent access to 9 major US telecommunications carriers despite multiple remediation attempts. Senate Commerce Committee testimony in December 2025 confirmed Verizon, AT&T, and T-Mobile cannot prove eradication. Intelligence collection continues with potential for future disruption.

9 carriers compromised

THREAT ATTRIBUTION



● Russia 49% ● China 14% ● Unknown 21% ● Iran 3% ● Other 13%

TOP 5 ACTORS BY SECTOR SPREAD

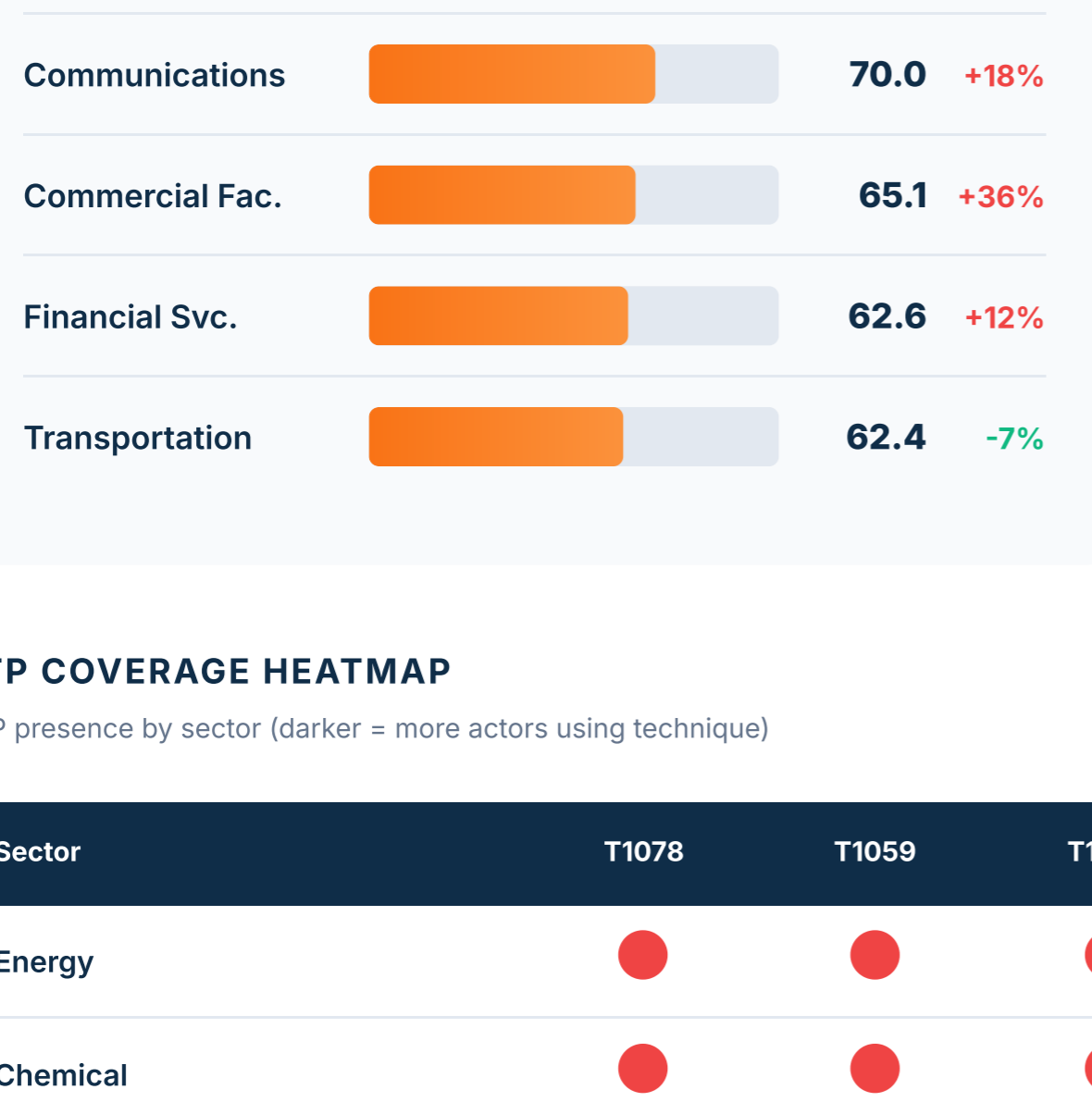


SECTOR RISK & TTP CONVERGENCE

ITR Scores & Attack Patterns Across 16 Sectors

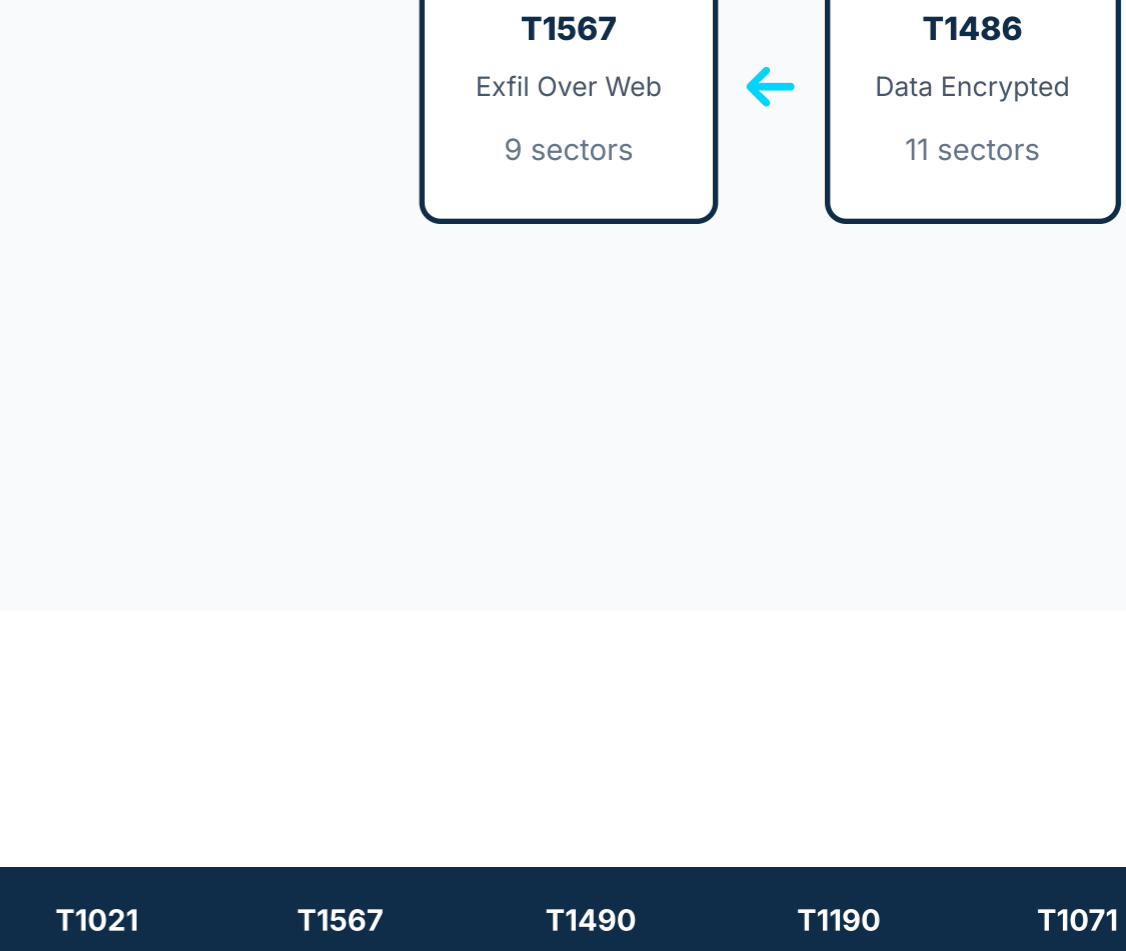
INTRUVENT THREAT RATING: TOP 8 CI SECTORS

Higher score = higher threat | Colored by risk level



UNIVERSAL ATTACK CHAIN

Most common TTP sequence observed across all sectors



TTP COVERAGE HEATMAP

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

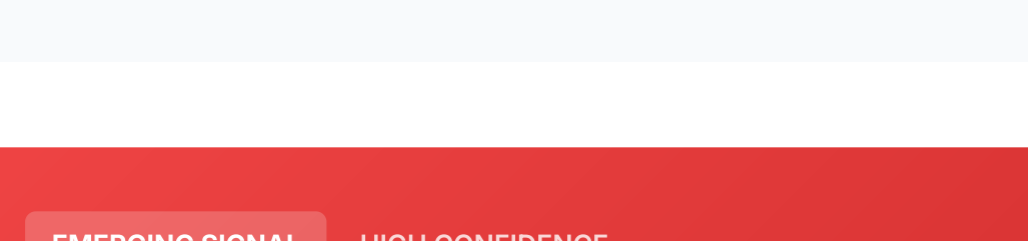
Heatmap table showing TTP coverage across 16 sectors for actors T1078, T1059, T1486, T1021, T1567, T1490, T1190, T1071

KEY INSIGHT T1078 (Valid Accounts) is present in ALL 16 sectors with 50 actors using it. Focus defensive investments on credential security — MFA, privileged access management, and credential monitoring should be top priorities.

05 CVEs & INCIDENT INTELLIGENCE

81 Incidents Across 16 Sectors

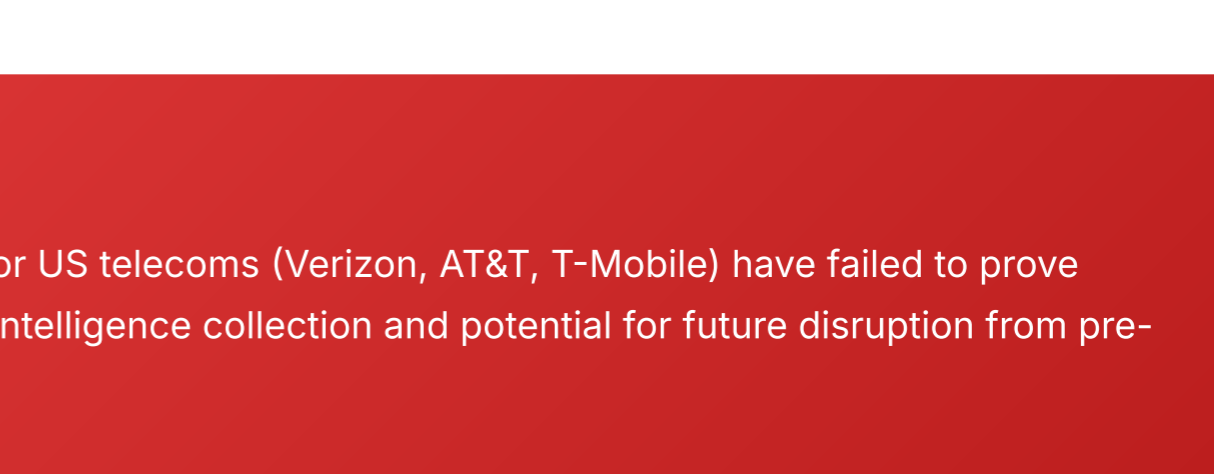
CVE SEVERITY DISTRIBUTION (46 CVEs)



Priority CVEs: CVE-2025-0282 Ivanti (9.0), CVE-2025-22457 Ivanti (9.0), CVE-2024-23113 Fortinet (9.8)

ITR SCORE BREAKDOWN: CROSS-SECTOR AVERAGES

Average dimension scores across 16 CI sectors



EMERGING SIGNAL HIGH CONFIDENCE Salt Typhoon Persistence Unresolved: Senate experts confirm 9 major US telecoms (Verizon, AT&T, T-Mobile) have failed to prove Chinese hackers have been eradicated from their networks. Ongoing intelligence collection and potential for future disruption from pre-positioned access continues.

Source: US Senate Commerce Committee, December 2025

06 EMERGING SIGNALS & EXECUTIVE ACTIONS

Critical Threat Signals Across 16 CI Sectors

EMERGING THREAT SIGNALS

Grid of 6 emerging threat signals: Supply Chain Cascade, Container-to-Hypervisor Chains, AI-Enabled Attacks, Ransom Calibration via Policy Theft, OT/ICS Exposure, AI/ML Infrastructure Targeting

TREND INDICATORS

Grid of 6 trend indicators: APT CI Targeting (+136%), Malware Email Surge (+131%), Access Broker Surge (+50%), Govt Ransomware Surge (+235%), Ransom Payments Drop (-35%), Voice Phishing Explosion (+442%)

THREE THINGS TO KNOW

Three key findings: 1. TELECOM COMPROMISED (9 major carriers), 2. CHINA EXPANDING (10 CI sectors), 3. CREDENTIALS UNIVERSAL (16/16 sectors)

QUICK WINS — DO THIS NOW: Enable MFA on VPNs, Patch CVE-2025-0282, Audit third-party/vendor access, Review OT/IT network segmentation, Test backup restoration procedures

BRACE Threat Intelligence CONTACT: contact@intruvent.com, 949-832-6925, www.intruvent.com

Get Sector-Specific Deep Dives: This cross-sector report covers high-level trends. For detailed Defend, Detect, and Hunt guidance tailored to your sector, explore our Deep Dive reports. Explore BRACE ->