

## Cyberattacks remain relentless as India record 505 threats a minute: Report

Education, healthcare and manufacturing bear brunt as Maharashtra leads in detections amid rise of 'cognitive intrusions' forecast for 2026



*Credits: Getty Images*

The latest findings by Quick Heal's 2026 Seqrite Threat Report suggest that India's cyber threat landscape is being shaped by increasingly automated, AI-assisted, and cross-platform attacks. India's cyber threat landscape saw sustained and large-scale activity between October 2024 and September 2025, with 265.52 million detections recorded across more than 8 million endpoints, translating to an average of 505 detections per minute. The volume of detections remained consistent throughout the year, indicating continuous threat activity rather than isolated spikes.

Malware distribution continued to be dominated by high-volume categories. Trojans accounted for approximately 43% of detections, while file infectors contributed around 35%, together forming nearly 70% of all recorded incidents. These threats were primarily delivered through phishing attachments, compromised websites, and pirated software, with infectors persisting in environments with unpatched systems and legacy infrastructure.

Behaviour-based detection systems, including next-generation antivirus and anti-ransomware engines, identified over 34 million anomalous threats during the period. At the same time, signature-based detections exceeded 230 million, reflecting the continued prevalence of traditional malware distribution methods. Cryptojacking detections reached approximately 6.5 million, indicating a shift toward stealth-based monetisation methods.

## Sectoral and geographic distribution

Education, healthcare, and manufacturing sectors together accounted for nearly 47% of total detections, highlighting their exposure due to large endpoint networks and operational dependencies. At a regional level, Maharashtra recorded the highest number of detections at over 36 million, followed by Gujarat with over 24 million and Delhi with more than 15 million detections. Major urban centres including Mumbai, New Delhi, and Kolkata reported the highest incident density.

Ransomware activity remained comparatively low in volume but significant in impact. It accounted for less than 1% of total detections, with activity peaking in January 2025 at 185 incidents and over 113,000 detections. Campaigns such as Xelera and Weaxor contributed to this surge. Detection levels declined in subsequent months but remained stable, indicating continued activity throughout the year.

Network-based exploits exceeded 9.2 million scans, with attackers targeting widely used systems such as WordPress plugins, Apache Tomcat, and SysAid platforms. Host-based exploits, particularly those using Windows shortcut files, recorded over 8 million detections, reflecting continued exploitation of simple attack vectors.

“Looking ahead, Seqrite forecasts that 2026 will usher in the era of cognitive intrusions, where adversaries leverage AI to automate reconnaissance, deception, and persistence. The threat battlefield will evolve from code-based to context-aware attacks, demanding defenses that are predictive, autonomous, and intelligence-led,” the report stated.