India logged 265 million cyber attacks in a year, reports Seqrite in its India Cyber Threat Report 2026

Seqrite released its India Cyber Threat Report 2026, outlining one of the most active cyber threat periods observed in the country. The report, developed by Seqrite Labs, which monitors more than 8 million endpoints, provides an assessment of threat activity between October 2024 and September 2025.

During this period, Seqrite recorded 265.52 million detections, averaging more than 727,000 detections per day and 505 detections every minute. Trojans and file infectors remained the most common categories, with 88.4 million Trojan detections and 71.1 million file infector detections, together accounting for nearly 70% of all observed attacks.

Next-generation antivirus (NGAV) and anti-ransomware engines detected over 34 million anomalous activities. Ransomware activity peaked in January 2025, with 185 incidents and 113,000 detections documented. Cryptojacking detections reached 6.5 million, while network-based exploit scans exceeded 9.2 million, frequently targeting systems running WordPress plugins, Apache Tomcat and SysAid.

Geographic and sectoral insights

Among states, Maharashtra (36.1 million detections), Gujarat (24.1 million) and Delhi (15.4 million) registered the highest volumes. Mumbai, New Delhi and Kolkata were the most targeted cities.

From an industry standpoint, education, healthcare and manufacturing collectively represented nearly 47% of detections—sectors that are both essential and often constrained in cyber defence resources.

Complementing the threat data, Seqrite's India Cybersecurity Preparedness 2026 Survey reported an average maturity score of 6.37/10 across organisations. While adoption of advanced malware protection (86.7%) and backup readiness (78.5%) was high, maturity gaps persisted in incident response, configuration management and asset hygiene.

New enterprise services launched

In response to the findings, Seqrite has introduced two enterprise-focused services:

Ransomware Recovery as a Service (RRaaS)

A recovery service designed to support organisations after ransomware incidents. It uses forensic-grade methods—such as cryptanalysis, isolated recovery workflows and custom tooling—to restore encrypted files while minimising reinfection risks.

Seqrite Digital Risk Protection Services (DRPS)

A SaaS platform for monitoring and mitigating digital risks outside traditional IT perimeters. The service uses machine learning to track fake accounts, counterfeit listings, domain spoofing and misuse of intellectual property across marketplaces, social media and the dark web. Automated, audit-ready reports support investigations, while Seqrite's "war room" facilitates takedowns and legal escalations.

Dr Sanjay Katkar, Joint Managing Director of Quick Heal Technologies, said the report is intended to help policymakers and enterprises understand evolving risks. He added that the introduction of RRaaS and DRPS aims to strengthen organisational resilience as cyber threats continue to intensify.

Threat forecasts and guidance

The report also highlights trends in advanced persistent threat activity, zero-day vulnerabilities, ransomware campaigns and malware families. Seqrite notes that 14 of the 20 predictions made in its previous report materialised, underscoring the increasing predictability of attack patterns in the Indian context.

The 2026 edition provides recommendations across areas such as predictive threat intelligence, identity-centric defence, AI security hardening, automated patching and resilience frameworks. It also emphasises cross-industry collaboration and continuous workforce training as essential components of enterprise cyber readiness.