Business Standard

India saw 265 mn cyber attacks, rising malware threats, says report

Seqrite Lab found ransomware activity peaked in January 2025, with 185 incidents and 1,13,000 detections

Cyber security firm Quick Heal's enterprise arm Seqrite has detected over 265 million attacks across 8 million endpoints or installed bases of its technology in India, the company said on Thursday.

The report, "State of Malware In India" compiled by Seqrite Labs, found that Maharashtra, with 36.1 million threat detections, Gujarat (24.1 million), and Delhi (15.4 million) emerged as the most affected states, with Mumbai, New Delhi, and Kolkata identified as the top targeted cities.

"We operate from close to 80 lakh plus endpoints. And these 80 lakh endpoints are deployed not only across the breadth of our nation, but also across 76 other countries. Between October 2024 and September 2025, Seqrite Labs monitored more than 80 lakh endpoints and recorded 265.52 million detections," a company official said.

The official said that the data on attacks is based on endpoints deployed in India.

"These 265 million attacks QuickHeal and Seqrite were able to block. We were able to prevent those attacks from impacting the endpoints on which our products were deployed," the officer said.

Seqrite Lab found ransomware activity peaked in January 2025, with 185 incidents and 1,13,000 detections.

"From an industry perspective, the education, healthcare, and manufacturing sectors together accounted for nearly 47 per cent of all detections, reflecting their criticality and resource constraints that make them vulnerable to large-scale attacks," the report said.

The officer said India's overall cybersecurity preparedness remains uneven, leaving organisations vulnerable to modern and fast-evolving threats.

The maturity of enterprises for cyber security in the country has improved in terms of taking back-up of data and storing it at different locations and frequently updating systems and implementing software patches, he added.

However, the maturity level continues to remain lowest when it comes to response to a cyber incident due to a lack of a well-defined plan.