THE TIMES OF INDIA

India records 265 million cyber attacks in 2025: Report

India faced over 265 million cyberattacks in 2025, with Trojans and file infectors dominating threats. Maharashtra, Gujarat, and Delhi were most impacted. Seqrite's new report highlights these alarming trends and introduces Digital Risk Protection and Ransomware Recovery services to combat escalating cyber threats across key sectors like education, healthcare, and manufacturing.

 L to R: Sudhanshu Tripathi - VP - Marketing, Jaswinder Singh- Director- Seqrite Labs, Vinayak Godse, CEO-DSCI, Samuel Sathyajith - Senior VP- Enterprise Sales, Ashish Pradhan - Chief Technology Officer, and Lalit Mohan -...

The enterprise arm of global cybersecurity solutions provider Quick Heal Technologies Limited, Seqrite, has released the India Cyber Threat Report 2026. The report claimed that the country recorded more than 265 million cyberattacks in 2025. The company has also announced two enterprise grade services that respond to one of the most intense threat phases the country has ever faced. The report has been developed by Seqrite Labs, India's largest malware analysis center, and presents a clear picture of a threat landscape that is accelerating at a pace that affects every sector. Here are some of the key highlights:

India Cyber Threat Report 2026: Key highlights

- 265.52 million malware detections across over 8 million endpoints.
- ·Trojans and File Infectors account for 70% of all attacks.
- ·Maharashtra, Gujarat, and Delhi are the most affected regions.
- ·Mumbai, Kolkata, and New Delhi emerge as top targeted cities.
- ·Education, Healthcare and Manufacturing account for nearly 47% of all detections.

Apart from this, Seqrite has also announced two enterprise grade services that respond to cyberattacks. Here are the details:

Seqrite Digital Risk Protection Services (Seqrite DRPS):

Continuous and comprehensive scanning across all web layers to detect threats ML-driven monitoring of social platforms for brand mentions, impersonation, and fraudulent activity Real-time monitoring and identification of exposed credentials and sensitive data Understanding brand perception and identifying negative or malicious sentiment trends Automated, audit-ready reports meeting regional data regulations with detailed digital evidence for investigations Dedicated DRPS war room ensuring swift takedowns, legal escalations, and crisis management

Seqrite Ransomware Recovery as a Service (Seqrite RRaaS)

Businesses regain data without funding attackers or risking further extortionQuick recovery ensures minimal downtime and operational bottlenecks Lower financial and reputational damage due to quick incident response Validated restoration prevents reinfection Detailed post-incident analysis helps strengthen defenses for the future