Delhi, Tamil Nadu, Telangana most affected by malware, says report

In response to the increasing threat landscape, Seqrite has introduced two advanced cybersecurity solutions.

Image used for representative purpose.

[Express News Service](#)

Updated on:
06 Dec 2024, 10:59 am
2 min read

NEW DELHI: Telangana, Tamil Nadu, and Delhi are the top three regions most affected by malware, according to the India Cyber Threat Report 2025. The report, published in collaboration with the Data Security Council of India (DSCI), also identifies the Healthcare, Hospitality, and BFSI (Banking, Financial Services, and Insurance) sectors as the most targeted by cybercriminals.

The report reveals that a staggering 369 million malware detections were recorded across an 8.44 million-device base, highlighting the extensive and growing scale of cyber threats in India. Notably, 85.44% of malware was detected using signature-based methods, which rely on identifying known malware patterns, while 14.56% were identified through behaviour-based detection, which flags suspicious activities even for new or unknown threats. The report further shows that Trojans (43.38%) and Infectors (34.23%) were the most commonly detected types of malware.

In response to the increasing threat landscape, Seqrite has introduced two advanced cybersecurity solutions. The Seqrite Malware Analysis Platform (SMAP) offers both static and dynamic analysis capabilities to evaluate suspicious files and URLs, providing a deeper level of threat detection.

"Our Threat Report delivers critical insights and actionable recommendations. SMAP empowers security professionals with advanced analysis tools, and Seqrite Threat Intel will provide real-time defense mechanisms," said Vishal Salvi, CEO of Quick Heal Technologies Limited.

Vinayak Godse, CEO of the Data Security Council of India, emphasized the growing importance of behavior-based detection, noting that the demand for this technology reflects a significant shift in both cyberattack strategies and defense mechanisms. "Attackers are now deploying more sophisticated ransomware that can bypass traditional signature-based

detection methods," he said. "I hope this report serves as a strategic compass for organizations and leaders in navigating the evolving threat landscape. We are pleased to collaborate with the Quick Heal team to present this comprehensive and nuanced understanding of India's cybersecurity challenges."