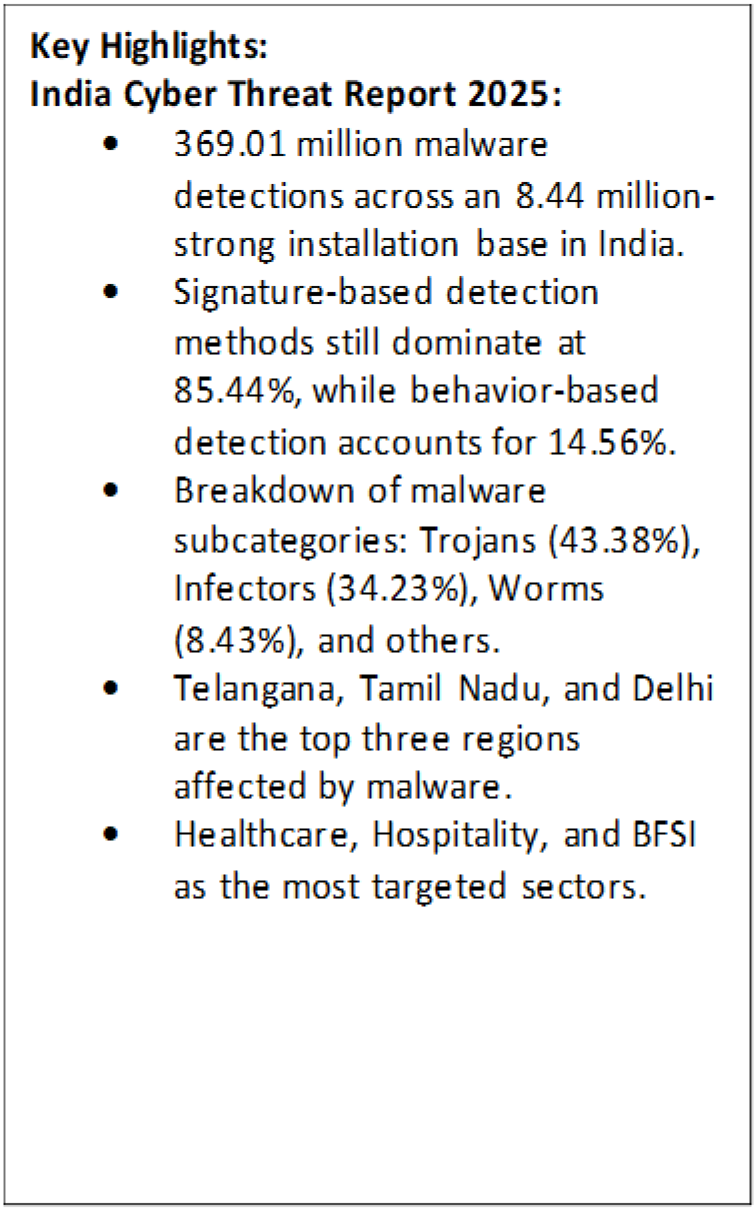
25 VARINDIA

DSCI and Seqrite Release 2025 Cyber Threat Report

Data Security Council of India (DSCI) in collaboration with Seqrite, the enterprise arm of global cybersecurity solutions provider, Quick Heal Technologies Limited, has today unveiled the second edition of the 'India Cyber Threat Report 2025'. The report was launched at the 19th edition of DSCI's Annual Information Security Summit (AISS) 2024.

The report provides an in-depth analysis of the current **cybersecurity** landscape in India, revealing alarming statistics and trends. The study identified a staggering 369 million malware detections across an installation base of 8.44 million in India, highlighting the scale and intensity of cyber threats facing the nation. Notably, 85.44% of detections relied on signature-based methods, while 14.56% came through behavior-based detection, emphasizing the need for adaptive security measures.



Key Highlights:

India Cyber Threat Report 2025:

- 369.01 million malware detections across an 8.44 million-strong installation base in India.
- Signature-based detection methods still dominate at 85.44%, while behavior-based detection accounts for 14.56%.
- Breakdown of malware subcategories: Trojans (43.38%), Infectors (34.23%), Worms (8.43%), and others.
- Telangana, Tamil Nadu, and Delhi are the top three regions affected by malware.
- Healthcare, Hospitality, and BFSI as the most targeted sectors.

The report breaks down malware subcategories, with Trojans leading at 43.38% of detections, followed by Infectors at 34.23%. The Android-based security detections reveal a concerning distribution of threats, wherein malware accounted for 42% of all detections, followed by Potentially Unwanted Programs (PUPs) as the second most common threat at 32%. Adware comprised 26% of detections in Android devices. The report also offers a state-wise analysis of malware detections, pinpointing Telangana, Tamil Nadu, and Delhi as the most affected regions. Furthermore, it sheds light on industry-specific vulnerabilities, identifying BFSI, Healthcare and Hospitality as the sectors most targeted by cybercriminals.

Vinayak Godse, Chief Executive Officer, Data Security Council of India, added, “The India Cyber Threat Report 2025 is an annual effort to bring out the big picture of India’s cyber threat landscape, providing insights at state, city, infrastructure and industry segment levels. The increase in the demand of behavior-based detections of malware represents an important evolution in both attack and defense strategies. This tells us that attackers are creating more sophisticated ransomware that can evade traditional signature-based detection methods. The report should serve as a strategic compass for organizations and leaders to navigate the threat landscape. We are glad to work with the Quick Heal team for collaborating to bring out the threat landscape in a comprehensive and nuanced manner.”

Vishal Salvi, Chief Executive Officer of **Quick Heal Technologies Limited,** commented, *“The unveiling of the 'India Cyber Threat Report 2025' alongside two unique solutions represent our comprehensive approach to addressing the evolving cybersecurity challenges faced by Indian businesses. This approach is not just about responding to threats but anticipating them. The Threat Report provides critical insights and actionable recommendations, while two solutions including Seqrite Malware Analysis Platform empowers security professionals with advanced analysis capabilities, and Seqrite Threat Intel will offer real-time defense mechanisms. I sincerely thank DSCI and our dedicated experts at the Labs for their relentless commitment to advancing excellence in cybersecurity and their efforts to reshape the ecosystem. These efforts ensure that our clients are always one step ahead in this digital arms race, fortifying India's cybersecurity landscape against current and future threats.”*

The report has come at a critical time as the cybersecurity landscape continues to evolve with emerging threats such as AI-driven attacks, cloud vulnerabilities, and sophisticated ransomware campaigns targeting critical infrastructure.