THE HINDU businessline.

Telangana, Tamil Nadu, Delhi are most affected regions of malware - Report

The study identified a staggering 369.01 million malware detections across an installation base of 8.44 million in India, highlighting the scale and intensity of cyber threats facing the nation

Telangana, Tamil Nadu, and Delhi are the most affected regions of malware and BFSI, Healthcare and Hospitality are the sectors most targeted by cybercriminals, said a report.

The study identified a staggering 369.01 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 per cent of detections relied on signature-based methods, while 14.56 per cent came through behaviour-based detection, emphasising the need for adaptive security measures, the report prepared by Data Security Council of India (DSCI) in collaboration with Seqrite, the enterprise arm of global cybersecurity solutions provider, Quick Heal Technologies has said.

The report titled -- 'India Cyber Threat Report 2025' -- broke down malware subcategories, with Trojans leading at 43.38 per cent of detections, followed by Infectors at 34.23 per cent.

The Android-based security detections reveal a concerning distribution of threats, wherein malware accounted for 42 per cent of all detections, followed by Potentially Unwanted Programs (PUPs) as the second most common threat at 32 per cent, the report highlighted.

It further said that Adware comprised 26 per cent of detections in Android devices.

“The increase in the demand of behaviour-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,” Vinayak Godse, Chief Executive Officer, DSCI, said.

The report should serve as a strategic compass for organisations and leaders to navigate the threat landscape, he added.

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.

“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,” Vishal Salvi, Chief Executive Officer of Quick Heal Technologies, said.