11 cyber threats every second: India’s digital expansion fuels attack surface

Updated - December 23, 2024 at 03:17 PM. | Hyderabad

Telangana, Tamil Nadu hits the charts with highest number of malware attacks: DSCRI-Seqruit report 369 million threats and counting; one million ransomware attacks cripple businesses in 2024

BY K V KURMANATH

India is facing unprecedented cyberattacks, with over 369 million threats detected in 2025 alone. Critical sectors such as healthcare, hospitality, and BFSI are in the crosshairs, with government entities also facing persistent threats.

This alarming surge, highlighted in the latest India Cyber Threat Report 2025 prepared by the Data Security Council of India (DSCI) and cybersecurity solutions company Seqruite, reveals a rapidly evolving threat landscape where cybercriminals are deploying increasingly sophisticated tactics.

The geographical distribution of cyberattacks in India reveals a concerning shift. While major tech hubs like Telangana (15.03 per cent) and Tamil Nadu (12 per cent) continue to face the brunt of malicious activity, a worrying trend is emerging in Tier 2 cities. This suggests that cybercriminals are casting a wider net and exploiting potentially weaker cybersecurity infrastructures in smaller urban centers.

The reports finds that on average, every minute sees 702 potential security threats. To put this in perspective, this is roughly equivalent to having 11 new cyber threats emerging every second somewhere in the country. This volume of attacks demonstrate the relentless nature of modern cyber threats and the constant pressure on security systems.

“As cyber criminals develop increasingly complex and diverse malware, the need for behavior-based detection technologies becomes crucial,” warns Vinayak Godse, CEO of the DSCI, said.

The report’s findings echo this concern, indicating a significant rise in behavior-based detections, as traditional signature-based systems struggle to keep pace with new malware variants.

Sanjay Katkar, Joint Managing Director of Quick Heal Technologies (Seqrite is the enterprise solution arm of Quick Heal Technologies), points to escalating geopolitical tensions and major national events as catalysts for these attacks.

“We’ve also observed an increase in sophisticated threats targeting sectors like Healthcare, Hospitality and BFSI, while government entities remain prime targets as well,” he said.

The report also reveals a staggering 1 million ransomware attacks over the year, underscoring the severity of the situation.

“India’s rapid digital expansion has significantly enhanced connectivity and technological adoption across various sectors, concurrently expanding the attack surface and increasing susceptibility to cyber threats,” the report said.

“The healthcare industry’s position as the most attacked sector (21.82 per cent of all attacks) is particularly concerning. This likely reflects the high value of medical data and the critical nature of healthcare systems, which might make organisations more likely to pay ransoms,” the report said.

The significant targeting of hospitality (19.57 per cent) and banking sectors (17.38 per cent) suggests that attackers are focusing on industries that handle large volumes of personal and financial data.

The rise in cloud-based detections is especially significant, with 62 per cent of detections occurring in cloud environments. This reflects the broader digital transformation across Indian businesses, but it also highlights a critical security challenge.

“As more organisations move their operations to the cloud, they create new opportunities for attackers to exploit misconfigured or inadequately protected cloud resources,” it said.