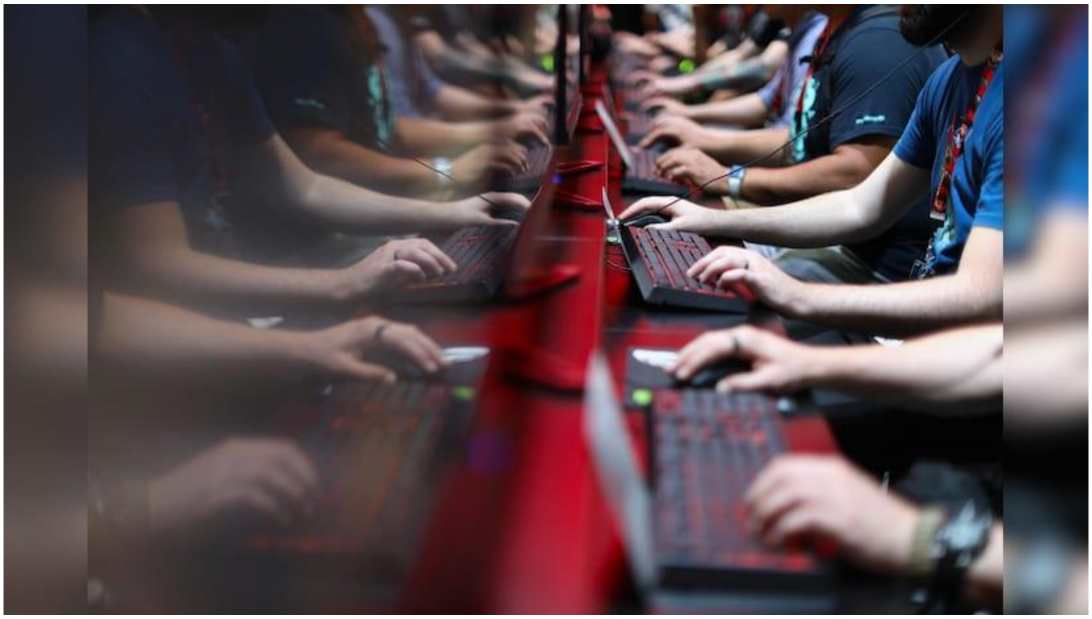
THE ECONOMIC TIMES | tech
English Edition ▾ | Today's ePaper

AI-driven, deepfake-enabled cyberattacks to increase in 2025: Report

The India Cyber Threat Report 2025 by the Data Security Council of India (DSCI) and Seqrite, spotlighted the evolving tactics of cybercriminals and the rise of AI-driven attacks as a major concern



AI-driven and deepfake-enabled cyberattacks are anticipated to become increasingly prevalent in 2025 with sectors like healthcare and finance most prone targets, according to a recent report.

The India Cyber Threat Report 2025 by the Data Security Council of India (DSCI) and Seqrite, spotlighted the evolving tactics of cybercriminals and the rise of AI-driven attacks as a major concern.

"Artificial Intelligence (AI) will be used to develop highly sophisticated phishing campaigns utilising deepfake technology and personalized attack vectors, making them harder to detect. AI-driven malware will adapt in real-time to evade traditional security measures, while data poisoning attacks will compromise the integrity of critical AI systems in sectors such as healthcare and autonomous transportation," the report noted.

Deepfake technology will create compelling malicious content, including fake video or audio messages from trusted sources. This will facilitate more effective social engineering attacks, making it easier for cybercriminals to deceive users into executing malware or revealing sensitive information, it added.

The integration of AI capabilities with vulnerabilities in supply chains will lead to new types of cyber threats.

Cybercriminals will employ AI-driven methods to execute intricate attacks, taking advantage of compromised development resources and hardware manufacturing processes to insert malicious code through corrupted libraries and embedded hardware, it said.

As AI tools become more accessible, attackers can automate and scale their operations, making it easier to target a wider range of victims. The report said this trend will likely lead to a surge in ransomware attacks, where malicious actors demand payment for the restoration of compromised data.

The rise of internet devices will open new avenues for cybercriminals to develop large-scale botnets. Vulnerabilities in poorly secured devices will be exploited to carry out Distributed Denial-of-Service (DDoS) attacks, which could disrupt essential services in industries such as manufacturing and healthcare that depend on edge computing, it said.

"Critical infrastructure sectors in India, including healthcare, finance, and energy, will remain prime targets for cybercriminals. These attacks will aim to disrupt services, steal sensitive data, and exploit geopolitical tensions, emphasizing the need for robust security frameworks and continuous monitoring to protect essential services," the report, which studied over 18 industry sectors, said.

Furthermore, the convergence of fake government service applications and fraudulent investment platforms will create hybrid threats in 2025, it said.

Cybercriminals will create advanced applications that mimic government benefit systems and investment services, using social engineering, influencer marketing, and sophisticated malware to carry out widespread financial fraud and identity theft, targeting public welfare recipients and retail investors alike.

Additionally, the rise of cryptocurrency mining will invite a surge in cryptojacking attacks, where malware hijacks computing resources to mine cryptocurrencies without the user's knowledge.

The changing threat landscape of 2025 requires CISOs to fundamentally rethink their cybersecurity strategies, the report said, adding that traditional security models are becoming ineffective against emerging quantum threats and AI-driven attacks.

It recommended embracing AI and ML (machine learning) for threat detection and response.

"The increasing complexity of cyber threats--such as zero-day exploits, polymorphic malware, and advanced persistent threats (APTs)--requires the automation and speed that AI-driven systems provide. CISOs should, therefore, prioritise...adopting AIenhanced security operations...leveraging ML for predictive threat intelligence...automating incident response," it said.

The report advocated for a focus on not just prevention, but cyber resilience, as the need of the hour.

"The cyber threat landscape is constantly evolving, and organizations must remain vigilant to protect themselves from emerging threats. Therefore, it is very important for the enterprises to strengthen their detection capabilities, incident response and focus on cyber resiliency. By adopting a proactive approach to cybersecurity, organisations can mitigate risks and safeguard their critical assets," said Sangamesh S, VP and Head of Seqrite Labs.

The report, which was launched at the 19th edition of DSCI's Annual Information Security Summit (AISS) 2024, surveyed 204 organisations and their C-suite executive. DSCI is a not-for-profit, industry body on data protection in India, set up by nasscom. Seqrite is the enterprise arm of cybersecurity firm Quick Heal Technologies.